

JP2000307588A

**OPTICAL SUBSCRIBER LINE TERMINATING DEVICE AND OPTICAL SUBSCRIBER END STATION
DEVICE**

Publication number : JP2000307588A

Date of publication of application : 02.11.2000

Application number : 11-109687

Applicant : FUJITSU LTD

Date of filing : 16.04.1999

Inventor : KADOSAWA TAKASHI
MIURA KENJI
MATSUO TAMOTSU
SHIONO HIDEKI
TOYODA YOSHIMI
KOYANAGI TOSHINORI
ABIRU SETSUO
YASUSATO ATSUSHI
FUJIYOSHI SHINICHI
UCHIDA KAZUHIRO
RYU KAZUYA
HIRASHIMA KATSUHIKO
YOTSUMARU TAKEO
WAKAYOSHI MITSU HARU
SAKAI TOSHIYUKI

Abstract:

PROBLEM TO BE SOLVED: To efficiently execute the receiving control and decoding processing of information.

SOLUTION: A first storing means M11a stores ciphering setting information which is being used presently. A second storing means M11b stores newly updated ciphering setting information. A ciphering setting information storing means 11 includes the means M11a and the means M11b, executes storage control on the means M11a and the means M11b. A ciphered information deciphering processing means 12 receives an information stream having a frame constitution and then validates stored ciphering setting information from the next frame to execute deciphering processing to a ciphered information part shown by ciphering setting information from the next frame.

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 12/28		H 0 4 L 11/20	D 5 J 1 0 4
H 0 4 B 10/00		H 0 4 B 9/00	B 5 K 0 0 2
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B 5 K 0 3 0
9/16			6 4 3 5 K 0 3 3
12/44		11/00	3 4 0 5 K 0 6 9

審査請求 未請求 請求項の数29 O L (全 44 頁) 最終頁に続く

(21) 出願番号 特願平11-109687

(22) 出願日 平成11年4月16日 (1999.4.16)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番1号

(72) 発明者 門澤 敬

大阪府大阪市中央区城見2丁目2番6号
富士通関西デジタル・テクノロジー株式会社内

(74) 代理人 100092152

弁理士 服部 毅哉

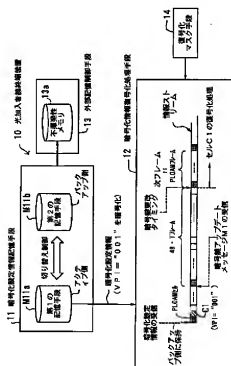
最終頁に続く

(54) 【発明の名称】 光加入者線終端装置及び光加入者線端局装置

(57) 【要約】

【課題】 情報の受信制御及び復号化処理を効率よく行う。

【解決手段】 第1の記憶手段M11aは、現在使用中の暗号化設定情報を記憶する。第2の記憶手段M11bは、新しく更改された暗号化設定情報を記憶する。暗号化設定情報記憶手段11は、第1の記憶手段M11aと第2の記憶手段M11bを含み、第1の記憶手段M11a及び第2の記憶手段M11bへの記憶制御を行い、暗号鍵の暗号鍵更改タイミングで、第1の記憶手段M11aと第2の記憶手段M11bとの切り替え制御を行う。暗号化情報復号化処理手段12は、フレーム構成を持つ情報ストリームを受信した後、記憶している暗号化設定情報を次フレームから有効にして、暗号化設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う。



【特許請求の範囲】

【請求項1】 光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置において、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報を対し、現在使用中の暗号化設定情報を記憶するアクティブ側の第1の記憶手段と、新しく更改された暗号化設定情報を記憶するバックアップ側の第2の記憶手段とを含み、前記第1の記憶手段及び前記第2の記憶手段への記憶制御を行い、前記暗号鍵の暗号鍵更改タイミングで、前記第1の記憶手段と前記第2の記憶手段との切り替え制御を行う暗号化設定情報記憶手段と、フレーム構成を持つ前記情報ストリームを受信し、記憶している前記暗号化設定情報を、前記暗号鍵更改タイミング以後の次フレームから有効にして、前記暗号化設定情報が示す暗号化された前記情報部分に対する復号化処理を前記次フレームから行う暗号化情報復号化処理手段とを、を有することを特徴とする光加入者線終端装置。

【請求項2】 前記暗号化設定情報記憶手段は、前記暗号鍵更改タイミングで前記第1の記憶手段と前記第2の記憶手段とを切り替えた後、あらたにアクティブ側になった第1の記憶手段に記憶してある前記暗号化設定情報を、あらたにバックアップ側になった第2の記憶手段へコピーすることを特徴とする請求項1記載の光加入者線終端装置。

【請求項3】 前記暗号化設定情報記憶手段は、バックアップ側の第2の記憶手段へのコピー中に、あらたな暗号化設定情報を受信した場合は、前記コピーの終了後に前記あらたな暗号化設定情報を前記第2の記憶手段に記憶することを特徴とする請求項2記載の光加入者線終端装置。

【請求項4】 前記暗号化設定情報記憶手段は、読み出しポートが2つある前記第1の記憶手段及び前記第2の記憶手段を含むことを特徴とする請求項1記載の光加入者線終端装置。

【請求項5】 前記暗号化設定情報記憶手段は、前記暗号化設定情報を受信して、前記第1の記憶手段または前記第2の記憶手段へ正常に書き込んだか否かを検証し、正常に書き込んだ場合にのみ応答信号を返送することを特徴とする請求項1記載の光加入者線終端装置。

【請求項6】 前記暗号化設定情報を不揮発性メモリに記憶させる外部記憶制御手段をさらに有することを特徴とする請求項1記載の光加入者線終端装置。

【請求項7】 前記外部記憶制御手段は、受信した前記暗号化設定情報と、バックアップ側の前記第2の記憶手段に格納されている暗号化設定情報とを比較し、異なる暗号化設定情報のみ前記不揮発性メモリに記憶させることを特徴とする請求項6記載の光加入者線終端装置。

【請求項8】 前記外部記憶制御手段は、前記暗号化設定情報をメモリに記憶させ、電源断時に前記メモリから前記不揮発性メモリへ、一括して前記暗号化設定情報を記憶させることを特徴とする請求項6記載の光加入者線終端装置。

【請求項9】 前記外部記憶制御手段は、前記暗号化設定情報をメモリに記憶させ、電源断時に前記メモリから前記不揮発性メモリへ、更改された暗号化設定情報のみ記憶させることを特徴とする請求項6記載の光加入者線終端装置。

【請求項10】 前記暗号化設定情報記憶手段は、電源復旧時の立ち上げ準備状態の期間のみ、前記不揮発性メモリからの前記暗号化設定情報を受け付けることを特徴とする請求項6記載の光加入者線終端装置。

【請求項11】 前記暗号化設定情報記憶手段は、電源復旧時に、前記不揮発性メモリから読み出された前記暗号化設定情報、またはあらたに送信された暗号化設定情報の一方を選択して有効にすることを特徴とする請求項6記載の光加入者線終端装置。

【請求項12】 前記暗号化情報の復号化処理を行える運用状態から、他の状態へ遷移して、再度前記運用状態になった場合は、前記運用状態になった時から前記暗号鍵更改タイミングを受信するまでの期間の復号化処理をマックスする復号化マックス手段をさらに有することを特徴とする請求項1記載の光加入者線終端装置。

【請求項13】 光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置において、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報を記憶する暗号化設定情報記憶手段と、フレーム構成を持つ前記情報ストリームを受信し、記憶している前記暗号化設定情報を次フレームから有効にして、前記暗号化設定情報が示す暗号化された前記情報部分に対する復号化処理を前記次フレームから行う暗号化情報復号化処理手段と、を有することを特徴とする光加入者線終端装置。

【請求項14】 光加入者系システムに接続して、暗号鍵を用いて暗号化を行った情報部分を含む情報ストリームを送信する光加入者線端局装置において、受信装置へ前記情報ストリームを送信する際に、フラグの設定制御を行うフラグ設定制御手段と、

前記フラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報の送信制御を行う暗号化設定情報送信制御手段と、を有することを特徴とする光加入者線端局装置。

【請求項15】 前記フラグ設定制御手段は、初期暗号化フラグを有し、前記初期暗号化フラグを前記受信装置が停止状態でクリア、初期暗号化の完了時にセットすることを特徴とする請求項14記載の光加入者線端局装置。

置。

【請求項16】 前記フラグ設定制御手段は、初期暗号化の実行中を示す初期暗号化実行中フラグを有することを特徴とする請求項14記載の光加入者線端局装置。

【請求項17】 前記フラグ設定制御手段は、前記受信装置に対する前記暗号化設定情報の設定更改が失敗と判断した場合は、設定更改失敗フラグをセットすることを特徴とする請求項14記載の光加入者線端局装置。

【請求項18】 前記フラグ設定制御手段は、前記受信装置が状態落ちしたと判断した場合は、設定更改未完了フラグをセットすることを特徴とする請求項14記載の光加入者線端局装置。

【請求項19】 前記フラグ設定制御手段は、暗号化の更改周期中に暗号化更改中フラグをセットすることを特徴とする請求項14記載の光加入者線端局装置。

【請求項20】 前記フラグ設定制御手段は、前記暗号化設定情報の設定更改を行う際には、設定更改要求フラグをセットすることを特徴とする請求項14記載の光加入者線端局装置。

【請求項21】 前記フラグ設定制御手段は、1つの前記受信装置につき、1つの前記論理コネクションの更改に対して、前記設定更改要求フラグをセットすることを特徴とする請求項20記載の光加入者線端局装置。

【請求項22】 前記フラグ設定制御手段は、前記暗号化設定情報の設定更改実行中には、設定更改実行中フラグをセットすることを特徴とする請求項14記載の光加入者線端局装置。

【請求項23】 前記暗号化設定情報を前記受信装置へ再度送信する上書き処理を行う暗号化設定情報上書き手段をさらに有することを特徴とする請求項14記載の光加入者線端局装置。

【請求項24】 前記暗号化設定情報上書き手段は、優先度の高い他のメッセージの送信を行う場合は、前記上書き処理を待機させることを特徴とする請求項23記載の光加入者線端局装置。

【請求項25】 前記暗号化設定情報上書き手段は、前記暗号化設定情報の設定更改実行中には、前記上書き処理を待機させることを特徴とする請求項23記載の光加入者線端局装置。

【請求項26】 前記暗号化設定情報上書き手段は、タイマを有し、前記タイマに設定された周期にしたがって、前記上書き処理を行うことを特徴とする請求項23記載の光加入者線端局装置。

【請求項27】 前記タイマの周期は、外部から任意の値に設定されることを特徴とする請求項26記載の光加入者線端局装置。

【請求項28】 前記暗号化設定情報送信制御手段は、前記暗号化設定情報を複数回送信する場合には、1回目の前記暗号化設定情報の送信時のみ他メッセージと調停処理を行い、調停後は前記暗号化設定情報を一定間隔毎に

自動的に送信することを特徴とする請求項14記載の光加入者線端局装置。

【請求項29】 前記暗号鍵の暗号鍵更改タイミングで、前記暗号化設定情報の更改を開始する暗号化設定情報更改手段をさらに有することを特徴とする請求項14記載の光加入者線端局装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は光加入者線端装置及び光加入者線端局装置に関し、特に光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線端装置、及び光加入者系システムに接続して、暗号鍵を用いて暗号化を行った情報部分を含む情報ストリームを送信する光加入者線端局装置に関する。

【0002】

【従来の技術】近年、通信サービスの多様化は加速し、ビデオ・オン・デマンド、CATV、高速コンピュータ通信等の需要が拡大しつつある。このような大容量の通信サービスを低料金で提供するためには、加入者通信網を光化した光加入者系システムが不可欠である。

【0003】光加入者系システムとしては、1本の光ファイバを複数の加入者で共有するPDS (Passive Double Star) が提案されている。また、特に欧州を中心にPDS方式を採用したPON (Passive Optical Network) システムが注目されており、光ファイバを各家庭まで敷設するFTTH (Fiber To The Home) システムの実現に向けて開発が進んでいる。

【0004】また、このようなFTTHシステムの実現のためには、音声や動画などのリアルタイムの通信要求に対して、通信帯域や品質を保証するために、ATM (Asynchronous Transfer Mode) を利用したATM-PONの構築が、FSAN (Full Service Access Networks : 光通信事業を推進するために設立された国際的な通信業界団体) を中心に進められている。

【0005】図25はATM-PONシステムの構成を示す図である。加入者宅100a~100n内には、光バースト伝送を行うONU (Optical Network Unit : 光加入者線端装置) 101a~101nが配置され、局200内にはOLT (Optical Line Terminal : 光加入者線端局装置) 201が配置される。

【0006】ONU101a~101nには電話機やCATV等が接続され、OLT201には交換機(ATM交換機、ISDN交換機等)202が接続する。また、ONU101a~101nとOLT201は、スターカプラ300と接続する。

【0007】局200から加入者宅100a~100nへの下り情報(下りセル)は、1本の光ファイバから、スターカプラ300を介して、樹枝状に分岐された光ファイバを通じて送信される。また、加入者宅100a~

100nから局200への上り情報(上りセル)は、樹枝状に分岐された光ファイバから、スターカプラ300を介して、1本に集約された光ファイバを通じて送信される。

【0008】このように、ATM-PONシステムは、スターカプラ300で局と複数の加入者とを1:nで接続して構成する、ATMを使った光分岐型のアクセスネットワークである。

【0009】ここで、OLT201からONU101a～101nへの下り通信は、放送型であるため、ITU-T勧告G.983では、ONU毎の秘匿性を目的として、暗号化(Churning)方式が規定されている。

【0010】まず、OLT201は、下りメッセージにより、ONU(例えば、ONU101a)に暗号鍵を要求する。すると、応答したONU101aは、暗号鍵を生成し、OLT201に通知する。

【0011】OLT201は、その暗号鍵を使用して、ONU101aに対して送信すべき下り情報に対して暗号化を施す。この下り情報の暗号化はVP(Virtual Path:仮想パス)毎に行われる。

【0012】この場合、OLT201は、ONU101aに対し、VPI(Virtual Path Identifier:仮想パス識別子)を単位として、どのVPに対して暗号化を施した(ON)か否か(OFF)を示す設定情報である暗号化設定情報を下りメッセージにより通知する。

【0013】このように、ATM-PONシステムの暗号化方式では、暗号鍵はONU毎に割り当てられ、下り情報の暗号化のON/OFFはVPI単位で行われる。そして、OLT201がONU101aに下りメッセージを用いて、暗号化設定情報を通知し、ONU101aでは自己の暗号鍵を用いて、暗号化されたVPの下り情報を復号化する。

【0014】

【発明が解決しようとする課題】しかし、上記のようなITU-T勧告G.983におけるATM-PONシステムの暗号化方式では、詳細な処理手順が規定されていない。

【0015】例えば、ONU101aでは、OLT201からの暗号化設定情報を保持しているが、ITU-T勧告G.983には復号化処理をいつ有効にするべきかが規定されていない。

【0016】したがって、OLT201側での暗号化処理、ONU101a側での復号化処理それぞれに時間的に大きなずれがあった場合などでは、暗号化・復号化が正常に行えないといった問題があった。

【0017】また、暗号化設定情報は、ONUの電源断時にはリセットされるため、電源復旧後は再度設定を行う必要があり、再立ち上げに時間がかかるなどといった問題もある。

【0018】このように、従来のATM-PONシステムの暗号化方式では、十分な技術が未だ確立されておらず、システム構築の実現のために高品質な通信制御を早急に確立する必要がある。

【0019】本発明はこのような点に鑑みてなされたものであり、高品質な通信制御を確立し、情報の受信制御及び復号化処理を効率よく行う光加入者線終端装置を提供することを目的とする。

【0020】また、本発明の他の目的は、高品質な通信制御を確立し、情報の送信制御を効率よく行う光加入者線終端装置を提供することである。

【0021】

【課題を解決するための手段】本発明では上記課題を解決するために、図1に示すような、光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置10において、論理コネクッション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報に対し、現在使用中の暗号化設定情報を記憶するアクティブ側の第1の記憶手段M11aと、新しく更改された暗号化設定情報を記憶するバックアップ側の第2の記憶手段M11bとを含み、第1の記憶手段M11a及び第2の記憶手段M11bへの記憶制御を行い、暗号鍵の暗号鍵更改タイミングで、第1の記憶手段M11aと第2の記憶手段M11bとの切り替え制御を行う暗号化設定情報記憶手段11と、フレーム構成を持つ情報ストリームを受信し、記憶している暗号化設定情報を、暗号鍵更改タイミング以後の次フレームから有効にして、暗号化設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う暗号化情報復号化処理手段12と、を有することを特徴とする光加入者線終端装置10が提供される。

【0022】ここで、第1の記憶手段M11aは、現在使用中の暗号化設定情報を記憶する。第2の記憶手段M11bは、新しく更改された暗号化設定情報を記憶する。暗号化設定情報記憶手段11は、第1の記憶手段M11aと第2の記憶手段M11bを含み、第1の記憶手段M11a及び第2の記憶手段M11bへの記憶制御を行い、暗号鍵の暗号鍵更改タイミングで、第1の記憶手段M11aと第2の記憶手段M11bとの切り替え制御を行う。暗号化情報復号化処理手段12は、フレーム構成を持つ情報ストリームを受信し、記憶している暗号化設定情報を、暗号鍵更改タイミング以後の次フレームから有効にして、暗号化設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う。

【0023】また、図15に示すような、光加入者系システムに接続して、暗号鍵を用いて暗号化を行った情報部分を含む情報ストリームを受信する光加入者線終端装置20において、受信装置へ情報ストリームを送信する際に、フラグの設定制御を行うフラグ設定制御手段21

と、フラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報の送信制御を行う暗号化情報送信制御手段22とを、有することを特徴とする光加入者線端局装置20が提供される。

【0024】ここで、フラグ設定制御手段21は、受信装置へ情報ストリームを送信する際に、フラグの設定制御を行う。暗号化設定情報送信制御手段22は、フラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報の送信制御を行う。

【0025】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図1は本発明の光加入者線終端装置の原理図である。光加入者線終端装置10は、ONUに該当し、ATM-PON等の光加入者系システムに接続してOLTから送信される情報ストリーム（複数のセルで構成される）を受信する。

【0026】そして、自己の装置で生成した暗号鍵を用いて、情報ストリーム内の暗号化された情報部分に対して復号化を行う。以降では、光加入者線終端装置10をONU10と呼ぶ。

【0027】暗号化設定情報記憶手段11は、暗号化設定情報を記憶するために、第1の記憶手段M11aと第2の記憶手段M11bの2面の記憶領域を有している。ここで、暗号化設定情報とは、論理コネクション毎に暗号化を施したか否かを示す設定情報である。具体的には、VPIを単位として、どのVPPに対して暗号化を施したか否かを示す設定情報のことをいう。

【0028】第1の記憶手段M11aは、アクティブ側であり、現在使用中（読み出し中）の暗号化設定情報を記憶している。第2の記憶手段M11bは、バックアップ側であり、新しく更改された暗号化設定情報を記憶する。

【0029】そして、暗号化設定情報記憶手段11は、第1の記憶手段M11aと第2の記憶手段M11bへの記憶制御（書き込み制御）を行い、暗号鍵の暗号鍵更改タイミング（古い暗号鍵を新しい暗号鍵に更改した時のタイミング）で、第1の記憶手段M11aと第2の記憶手段M11bとの切り替え制御を行う。詳細は後述する。

【0030】暗号化情報復号化処理手段12は、フレーム構成を持つ情報ストリームを受信し、記憶している暗号化設定情報を第1の記憶手段M11aから読み出して、暗号鍵更改タイミング以後の次フレームから、読み出した暗号化設定情報を有効にする。そして、暗号化設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う。

【0031】例えば、情報ストリーム中の1つのフレームの中で、VPI="001"（"001"はヘキサデ

ータ）の情報が暗号化されている旨が暗号化設定情報に記載されているものとする。また、VPI="001"に対応するセルがC1だとする。

【0032】図に示すように、暗号化設定情報を受信すると、バックアップ側の第2の記憶手段M11bに記憶する。その後、暗号鍵アップデートメッセージM1を受信して、48×Tフレーム経過した後の暗号鍵更改タイミング以後の次フレームからこの暗号化設定情報を有効にする。このようにして復号化処理の有効タイミングを明確に規定したので、暗号化処理、復号化処理の不一致を防止することが可能になる。なお、詳細動作は後述する。

【0033】外部記憶制御手段13は、暗号化設定情報を不揮発性メモリ13aに記憶させる。復号化マスク手段14は、暗号化情報の復号化を行える運用状態から、他の状態へ遷移して再度運用状態になった場合に、運用状態になった時から暗号鍵更改タイミングを受信するまでの期間の復号化処理をマスクする。なお、外部記憶制御手段13及び復号化マスク手段14の詳細については後述する。

【0034】次に本発明のONU10の具体的な構成・動作について詳しく説明する。なお、以降では暗号化処理をChurn、復号化処理をDechurn、暗号化設定情報をChurned-VPP設定情報と呼ぶ。

【0035】図2は情報ストリームの構成及びChurned-VPP設定情報のフォーマットを示す図である。OLTから送信される情報ストリームの1つのフレーム（PLOAMフレーム）は、OLTとONU10間で制御情報を通信するためのPLOAM（Physical Layer Operation And Management）セルと、実際の通信情報であるユーザセルC1～C27から構成される。そして、このPLOAMフレーム2つ分で、Tフレームと呼ぶ（伝送レートが150Mbpsモードの場合）。また、PLOAMセル及びユーザセル共に、1セルが53バイトである。

【0036】Churned-VPP設定情報は、PLOAMセルで送信される各種制御情報のうちの1つであり、PLOAMセルの40バイト～51バイトまでがChurned-VPP設定情報として定義されている。

【0037】40バイト目は、PON-IDであり、ONU10の識別子としてPON-IDが記される。41バイト目は、Churned-VPP設定情報であることを知らせる識別子が記される。この識別子は"00001111"（左側がMSB、右側がLSBである。以降同様）である。

【0038】43、44バイト目は、VPIを示す情報であり、43、44バイト目に記されるVPI情報をVPI[11:0]と表す。また、43バイト目の"a b c d e f g h"をVPI[11:4]と表し、44バイト目の"i j k l"をVPI[3:0]と表す。なお、

ATM-PONシステムのVPIの値は4096個ある(4096VPIある)。また、ユーザセルも、どのVPIから流れてきたものかを示すために、同様なVPI情報をそれぞれ個別に有している。

【0039】ここで、[M:N]は、下位Nビットから上位Mビットの(M-N+1)ビットのデータであることを意味する。42バイト目は、43、44バイト目に記されたVPIに対して、Churnされているか否かを示す情報が記される。内容は“xxxxxxxx”

(x=未定義)であり、a(フラグビット)=1ならChurnされており(したがって、ONU10ではDechurnしなければならない)、a=0ならChurnされていない。45～51バイト目は未定である。

【0040】図3は次フレームでDechurnを実現するためのブロック構成を示す図である。なお、Churned-VPメッセージフラグ設定手段11-1とChurned-VP設定情報書き込み手段11-2は暗号化設定情報記憶手段11内に含まれ、復号化処理手段12は暗号化情報復号化処理手段12に対応する。

【0041】Churned-VPメッセージフラグ設定手段11-1は、PLOAMセルのChurned-VP設定情報を受信した場合に、Churned-VPメッセージフラグをセットする。

【0042】Churned-VP設定情報書き込み手段11-2は、Churned-VPメッセージフラグをライトインペールの1つとして用い、RAM11a(暗号化設定情報記憶手段11が含む記憶手段に対応する)にChurned-VP設定情報の書き込みを行う。RAM11aは、256アドレスであり、1アドレスが格納するデータ領域は16ビットある。

【0043】書き込み処理としては、VPI[11:0]のうち、VPI[11:4]の8ビットをRAM11aへの書き込みアドレスとし、aビット情報をRAM11aへの書き込みデータとする。

【0044】ここで、VPI[11:4]をRAM11aのアドレスとした場合に、この1つのアドレスに16ビットの格納領域があるため、1アドレスにVPI[3:0](4ビット)の16通りのVPI値を割り当てることができる。

【0045】すなわち、RAMの1つのアドレスに対して、16通りのVPIを設定でき、この16通りのVPIに対応するaビット情報を、RAM11aの格納領域である16ビットの各ビットに対してデータとして書き込んでいく。したがって、RAM11aは、4096個のaビット情報の記憶領域を有することになる。

【0046】復号化処理手段12は、情報ストリームを受信し、ユーザセルに記載されているVPI[11:0]を抽出する。そして、抽出したVPI[11:0]のVPI[11:4]をRAM11aへの読み出しアドレスとし、VPI[3:0]に対応する位置にあるビッ

トのaビット情報を読み出しデータとする。aビット情報は1ならば、そのセルを暗号鍵を用いてDechurnし、aビット情報は0ならば、NotDechurn(復号化を行わずスルー)とする。

【0047】図4は次フレームからDechurnを行う際のタイミングチャートを示す図である。情報ストリームのPLOAMセルaのChurned-VP設定情報に、VPI[11:0] = “001” (“001”はヘキサデータ)の情報がChurnされている(aビット情報は1)旨が記載されているものとする。

【0048】Churned-VPメッセージフラグ設定手段11-1は、PLOAMセルaを受信して、41バイト目のChurned-VP設定情報のIDを認識すると、Churned-VPメッセージフラグを図に示す位相で出力する。

【0049】また、Churned-VP設定情報書き込み手段11-2は、VPI[11:0] = “001”及びaビット情報(=1)を次フレームのユーザセルC1の区間まで内部でラッチする。

【0050】そして、Churned-VPメッセージフラグとPLOAMパルス(PLOAMセルの位置を示すパルス)との論理をとった信号をライトインペールとして、図に示すセルFP(セルの位置を示すパルス)の位置で、VPI[11:4] = “00”をRAM11aの書き込みアドレス、16ビットのVPI[3:0] = “1”の位置にaビット情報を書き込みデータとしてRAM11aに書き込む。

【0051】このように、PLOAMセルaを受信した後、次フレームのPLOAMセルbの先頭位置でPLOAMセルaにあったChurned-VP設定情報をRAM11aに書き込み、その後、復号化処理手段12で読み出して、図に示す位置A(次フレームのユーザセルC1の先頭)からVPI[11:0] = “001”に対応するセルのDechurnを行っていく。ここではVPI[11:0] = “001”はセルC1としたので、位置AからセルC1のDechurnが行われる。

【0052】一方、情報ストリームのPLOAMセルbのChurned-VP設定情報に、VPI[11:0] = “010”とあり、Churnされていない(aビット情報は0)旨が記載されている場合には、図に示すようなタイミングでVPI[11:0] = “010”はNotDechurnとなる。

【0053】このように、本発明のONU10では、OLTがPLOAMセルに設定したChurned-VP設定情報を、次フレームにあるPLOAMセル以降から有効にするような構成とした。

【0054】これにより、次フレームのユーザセルから即時にDechurn処理を行うことができるので、暗号化処理と復号化処理の不一致防止、さらにデータ疎通時間を短縮させることが可能になる。

【0055】次に暗号鍵更改について説明する。本発明のONU10が適用されるATM-PONシステムでは、OLT側に位置する保守端末装置からの要求毎に、暗号鍵（以降、Churning-Keyと呼ぶ）の更改（鍵を新しくすること）を行っている。図5はChurning-Keyの更改シーケンスを示す図である。

【S1】OLTは、新しいChurning-Keyの送信要求として、Churning-KeyアップデートメッセージM1をONU10に送信する。

【S2】ONU10は、新しいChurning-Keyを生成して、ACKメッセージm1に乗せてOLTに返送する。

【S3】OLTは、Churning-KeyアップデートメッセージM1を送信してから16×Tフレーム経過した後、Churning-KeyアップデートメッセージM2をONU10に送信する。

【S4】ONU10は、ステップS2と同様に、ACKメッセージm2に更改したChurning-Keyの情報を乗せてOLTに返送する。

【S5】OLTは、Churning-KeyアップデートメッセージM2を送信してから16×Tフレーム経過した後、Churning-KeyアップデートメッセージM3をONU10に送信する。

【S6】ONU10は、ステップS2及びステップS4と同様に、ACKメッセージm3をOLTに返送する。

【S7】OLTがChurning-KeyアップデートメッセージM1をONU10へ送信してから48×Tフレーム経過した時点（Churning-Key更改タイミング）で、新しいChurning-Keyが使用される。すなわち、OLTはこの新しいChurning-KeyでChurnを行ひ、ONU10は新しいChurning-KeyでDechurnを行う。なお、16×Tフレームのカウントは、図に示すようにOLT、ONU10の双方で行う。

【0056】したがって、OLTがChurning-KeyアップデートメッセージM1をONU10に送信してから、48×Tフレーム経過するまでは、旧タイプのChurning-Keyを用いて、OLTとONU10間でChurn/Dechurnが行われる。

【0057】次に暗号化設定情報記憶手段11の2面RAM構成及びコピー動作について説明する。図5で説明したように、Churning-KeyをChurning-Key更改タイミングで更改した場合には、Churned-VP設定情報もこのタイミングでONU10側で更改しなければならない。したがって、Churning-Key更改タイミングとなる以前にOLTから送信された新しいChurned-VP設定情報を記憶しておく必要がある。

【0058】図6は2面RAMを持つONU10のブロック構成を示す図である。図3で説明した構成に対し

て、あらたにRAM11bと、切り替え制御手段11-3、コピー制御手段11-4が付加されている。切り替え制御手段11-3とコピー制御手段11-4は暗号化設定情報記憶手段11内に含まれる。

【0059】最初、RAM11aを、アクティブ側（VPI[11:4]をアドレスとして現在Churned-VP設定情報が読み出されているRAM）とし、RAM11bをバックアップ側（OLTから送信された新しいChurned-VP設定情報を次のChurning-Key更改タイミングまで保持しておくRAM）とする。

【0060】切り替え制御手段11-3は、Churning-KeyアップデートメッセージM1～M3を3回受信して、Churning-KeyアップデートメッセージM1から48×Tフレーム経過した場合には、その時間をChurning-Key更改タイミングとして認識する。

【0061】そして、Churning-Key更改タイミングでRAM11aとRAM11bを切り替えて、RAM11bをアクティブ側、RAM11aをバックアップ側とする。

【0062】一方、このままでは古いChurned-VP設定情報を記憶しているRAM11aがバックアップ側となってしまう。したがって、コピー制御手段11-4は、新しくアクティブ側になったRAM11bからデータをRAM11aへコピーしていく。

【0063】なお、RAM11a及びRAM11bは共に読み出しポートを2つ有している。このため、例えば、アクティブ側のRAMからバックアップ側のRAMへコピーが行われている最中でも、アクティブ側RAMからChurned-VP設定情報を読み出すことができる。

【0064】図7はコピー動作手順を示すフローである。なお、最初はRAM11aをアクティブ側、RAM11bをバックアップ側とし、RAM11aとRAM11bのそれぞれは、図に示すような値（例えば、“000”=1とは、VPI=“000”のaビット情報が1ということ）が格納されているものとする。

【S10】切り替え制御手段11-3は、Churning-Key更改タイミングでRAM11aとRAM11bを切り替える。

【S11】コピー制御手段11-4は、切り替え制御手段11-3から通知されたChurning-Key更改タイミングを受信すると、RAM11bに対する読み出しアドレスをインクリメントして、RAM11bからデータを読み出す。

【S12】コピー制御手段11-4は、RAM11aに対する書き込みアドレスをインクリメントして、RAM11bから読み出したデータをRAM11aへ書き込んでいく。

【S13】コピー制御手段11-4は、書き込みアドレスが最大になったか否かを判断する。最大でなければステップS11へ戻って、ステップS11、S12を繰り返していき、最大であればコピーを終了する。

【0065】図8はコピー動作時のタイミングチャートを示す図である。KEYTIMは、Churning-Key更改タイミングパルスである。RAM-STATEは、2面のRAMがアクティブ側かバックアップ側かを示す信号であり、図では更改前のRAMステートとしてRAM(B)がアクティブ側であり、更改後にRAM(A)がアクティブ側となるものとする。

【0066】COPYMODEは、コピー動作時に“H”となる信号である。COPYCTRは、COPYMODEが“H”の間、RAMの256アドレス数をカウントするための信号である。実際には、XWEが図に示すような位相となるので、259進カウンタを用いている。

【0067】RAMA-RADは、新しくアクティブ側になったRAM(A)の読み出しアドレスを示す信号であり、COPYCTRを1段ずらした信号を読み出しアドレスとして使用する。

【0068】RAMA-RDTは、RAMA-RADのアドレスで読み出された読み出しデータを示す信号であり、アドレス0に対して読み出しデータA、アドレス1に対して読み出しデータB、……である。RAMA-RADから1段ずれた位置に読み出しデータが出力される。

【0069】RAMB-WDTは、バックアップ側となったRAM(B)への書き込みデータを示す信号であり、RAMA-RDTを1段ずらした信号を書き込みデータとして使用する。

【0070】RAMB-WADは、RAMB-WDTをRAM(B)へ書き込むための書き込みアドレスを示す信号である。アドレス0に対して書き込みデータA、アドレス1に対して書き込みデータB、……をRAM(B)へ書き込んでいく(コピーする)。

【0071】XWEは、バックアップ側となったRAM(B)へ、RAM(A)の内容をコピーする場合の書き込みイネーブル信号であり、アクティブ“L”である。以上説明したように、本発明では、2面あるRAMの切り替えを行った場合に、新しいChurned-VP設定情報を、切り替え後にバックアップ側となったRAMへコピーする構成にしている。

【0072】これにより、バックアップ側も新しいChurned-VP設定情報を絶えず持つことができ、OLT側とのChurned-VP設定情報の不一致を防止することが可能になる。

【0073】次にコピー中にあらたなChurned-VP設定情報を受信した場合の動作について説明する。Churning-Key更改タイミングは、PLOA

M同期を最小単位として、フレーム数を数えているので必ずPLOAMセルの位置で上がることになる。

【0074】この場合、Churning-Key更改タイミングの位置のPLOAMセルがChurned-VP設定情報を持つセルの場合、バックアップ側のRAMへは、アクティブ側のRAMのデータのコピーが開始されているため、その情報をバックアップ側のRAMへ即時に書き込むことができない。

【0075】そこで、コピー中にこのようなChurned-VP設定情報を受信した場合には、フラグ(上述したCOPYMODEをフラグとして利用)をセットし、コピー終了後にフラグをクリアして、バックアップ側のRAMへ上書きする構成とする。

【0076】図9はコピー中にChurned-VP設定情報を受信した際の動作を示すタイミングチャートである。COPYMODEは、コピー動作時に“H”となる信号である。CHURNED-TRは、Churned-VP設定情報を受信したこと示すトリガ信号であり、受信時に“H”となる。

【0077】CHURNED-LTは、COPYMODEが“H”で、CHURNED-TRが“H”になった場合にCHURNED-TRをラッチした信号である。CVP-CTRは、CHURNED-LTの立ち下がりによって、バックアップ側のRAMへ書き込むための書き込みアドレスを示す信号である。

【0078】以上説明したように、コピー中に受信したChurned-VP設定情報に対しては、コピー終了後に書き込む構成とした。このように、コピーを優先して、その後を上書きすることにより、RAMへのコピー動作時のコピーエラーを防止することが可能になる。

【0079】次にChurned-VP設定情報を受信した際の応答信号の返送制御について説明する。ITU-T勧告G.983では、ONU10がChurned-VP設定情報を受信した場合、受信したことをOLTへ通知するための応答信号を返送する旨が規定されているが、返送条件については規定されていない。

【0080】したがって、本発明の暗号化設定情報記憶手段11は、Churned-VP設定情報を受信してRAMへ書き込んだ際に、再度読み出してペリファイチェック(書き込んだ値と読み出した値とを比較する)を行う。そして、正常に書き込んだ場合にのみ、ONU10はOLTへ応答信号を返送する。

【0081】図10は応答信号の返送制御手順を示すフローチャートである。RAM(A)をアクティブ側、RAM(B)をバックアップ側とし、コピー動作は終了しているものとする。

【0082】したがって、Churned-VP設定情報を受信した際には、RAM(B)へ書き込み、再度RAM(B)から読み出してペリファイチェックを行った後に応答信号の返送制御を行う。

〔S20〕Churned-VP設定情報を受信する。
〔S21〕Churned-VP設定情報が示すアドレスのデータをRAM (B) から読み出す。すなわち、VPI [11:4] のアドレスに対応するデータのVPI [3:0] の位置にあるデータ (a ビット情報) をRAM (B) から読み出す。

〔S22〕RAM (B) から読み出したデータのパリティチェック (LSI 間同士のデータ伝送などでは、データ送受信の信頼性確保のため、誤り訂正を行う必要がある)、誤り訂正符号をデータに付加して送受信を行っている) を行う。正常の場合はステップS23へ行く。パリティエラーの場合はステップS29へ行く。

〔S23〕RAM (B) から読み出したデータと、受信したChurned-VP設定情報のa ビット情報とを比較する。値が異なる場合はステップS24へ行き、値が同じ場合はステップS25へ行く。

〔S24〕ステップS21と同じアドレスへ、更改されたa ビット情報を書き込む。

〔S25〕ステップS21と同じアドレスからデータを再び読み出す。

〔S26〕RAM (B) から読み出したデータのパリティチェックを行う。正常ならばステップS27へ行く。パリティエラーの場合はステップS29へ行く。

〔S27〕RAM (B) から読み出したデータと、受信したChurned-VP設定情報のa ビット情報とを比較する。値が同じ場合はステップS28へ行き、値が異なる場合はステップS29へ行く。

〔S28〕RAM (B) へ正常に書き込んだので、Churned-VP設定情報を受信したことを通知するための応答信号をOLTへ返送する。

〔S29〕ONU10の全体制御を行っている全体制御部へエラー通知を送信する。

【0083】以上説明したように、本発明の暗号化設定情報記憶手段11は、Churned-VP設定情報を受信し、RAMへ書き込んだ際に正常に書き込んだ否かを検証する。そして、ONU10は、正常に書き込んだ場合にのみ応答信号を返送する構成である。これにより、OLT側とのChurned-VP設定情報の設定不一致を防止することが可能になる。

【0084】次に外部記憶制御手段13について説明する。本発明のONU10ではバックアップ電源を有しており、外部記憶制御手段13は、電源断時にはバックアップ電源を利用して、Churned-VP設定情報を不揮発性メモリ (フラッシュメモリなど) 13aに記憶させる。

【0085】これにより、電源断になっても不揮発性メモリ13aにChurned-VP設定情報を保持することができるので、電源復旧後に再度Churned-VP設定情報をOLTから送信要求しなくてもよい。

【0086】また、外部記憶制御手段13は、一旦、不

揮発性メモリ13aにChurned-VP設定情報を格納した後は、あらたに受信したChurned-VP設定情報と、バックアップ側のRAMに格納されているChurned-VP設定情報とを比較し、異なるChurned-VP設定情報のみを不揮発性メモリ13aに記憶させる。

【0087】具体的には、図10のステップS24で、更改されたa ビット情報を書き込んだ際に、a ビット情報が更改されていることを示す更改フラグを暗号化設定情報記憶手段11がセットする。

【0088】外部記憶制御手段13は、この更改フラグが立っている場合に、バックアップ側のRAMから、対応するアドレスのデータを読み出し、不揮発性メモリ13aへ記憶させる。このように、更改されたChurned-VP設定情報だけを記憶していくので効率よく不揮発性メモリ13aに記憶させることができる。

【0089】一方、不揮発性メモリ13aには書き込み回数が制限されているものが多いため、さらに書き込み回数を削減する工夫が必要である。したがって、外部記憶制御手段13では、電源復旧時にはChurned-VP設定情報を例えばSRAM (Static-RAM) 等のメモリに一旦記憶させ、電源断時にSRAMから不揮発性メモリ13aへ、一括してChurned-VP設定情報記憶させてもよい。これにより、不揮発性メモリ13aへのアクセス回数を削減することが可能になる。

【0090】また、一旦SRAMから不揮発性メモリ13aへ一括書き込みを行った初期動作以降は、更改フラグが立っているChurned-VP設定情報のみをSRAMへ書き込む。そして、電源断時にはSRAMから不揮発性メモリ13aへ、更改されたChurned-VP設定情報のみを記憶させてもよい。

【0091】図11は更改されたChurned-VP設定情報をSRAMから不揮発性メモリ13aへ記憶させる場合の処理手順を示すフローチャートである。

〔S30〕暗号化設定情報記憶手段11は、Churned-VP設定情報が更改されている場合は、更改フラグを立てる。

〔S31〕外部記憶制御手段13は、バックアップ側のRAMから、更改フラグにもとづいて対応するChurned-VP設定情報を読み出す。

〔S32〕外部記憶制御手段13は、更改されたChurned-VP設定情報をSRAMへ書き込む。

〔S33〕外部記憶制御手段13は、ONU10の電源断時に、SRAMに格納している情報を不揮発性メモリ13aへ書き込む。

【0092】このように、電源断時には、更改されたChurned-VP設定情報のみをSRAMから不揮発性メモリ13aへ記憶させてもよい。これにより、不揮発性メモリ13aへのアクセス回数をさらに削減することが可能になる。

【0093】次に電源復旧時のONU10の動作について説明する。ITU-T勧告G.983では、ONUの動作状態としてo1状態～o10状態を定めており、特にONUの電源復旧後の状態は、o1状態またはo9状態であることが規定されている。

【0094】o1状態とは、ONUの電源復旧後の初期状態のことである。o9状態とは、緊急停止状態であり、この状態になると、ONUはネットワークから切り離されて、通信ができなくなる。

【0095】また、本発明では、ONU10の電源復旧後の動作状態として、o1状態へ遷移させるべきか、またはo9状態へ遷移させるべきかを判断するための立ち上げ準備状態（以降、o0状態と呼ぶ）をあらたに設けることにした。

【0096】本発明の暗号化設定情報記憶手段11では、このo0状態を利用して、電源復旧時のo0状態の期間のみに、不揮発性メモリ13aからChurned-VP設定情報を受け付けることにする。

【0097】これにより、ONU10の運用状態（以降、o8状態と呼ぶ）中に、誤ってRAMに対する外部からの書き込みがあった場合でもその情報を有効としないので、OLT側とのChurned-VP設定情報の不一致を防止することが可能になる。

【0098】一方、暗号化設定情報記憶手段11は、o0状態の時に、不揮発性メモリ13aから読み出されたChurned-VP設定情報と、あらたに送信された暗号化設定情報とのいずれを有効にすべきか判断して選択することができる。

【0099】すなわち、ONU10は、o0状態時に不揮発性メモリ13aから再ロードしたChurned-VP設定情報を有効にするかどうかは未定とする。なぜなら、OLTから送信される、あらたなChurned-VP設定情報をONU10へ設定したい（有効としたい）場合があるからである。そこで、2面あるRAMのうち、一方を不揮発性メモリ13aからロードした値を持っておくRAM、他方をNotChurnにするためにイニシャライズ（以降、NotChurn設定と呼ぶ）をかけたRAMをo0状態時に設定しておく。

【0100】そして、不揮発性メモリ13aからロードした値を有効にしたい場合は、外部フラグをセットし、そのロードした値をRAMに保持させ、その後、受信したChurned-VP設定情報をこのRAMに上書きしていく。

【0101】また、外部フラグがセットされていない場合は、OLTからのChurned-VP設定情報を、NotChurn設定されたRAMへ書き込んでいく。それぞれの場合ともChurning-Key更改タイミングで、コピー動作が開始される。

【0102】図12は暗号化設定情報記憶手段11の電源復旧時の動作状態を示すフローチャートである。RA

M(A)をNotChurn設定されたRAMとし、RAM(B)を不揮発性メモリ13aからロードされたChurned-VP設定情報を保持するロード値設定RAMとする。なお、期間BではユーザセルはNotDechurnである。

【S40】外部フラグがセットされているか否かを判断する。セットしていればステップS41へ、セットしていなければステップS46へ行く。

【S41】RAM(A)をアクティブ側、RAM(B)をバックアップ側と設定する。

【S42】Churned-VP設定情報を受信した場合は、RAM(B)へ上書きする。

【S43】Churning-Key更改タイミングで、RAM(A)をバックアップ側、RAM(B)をアクティブ側に設定する。

【S44】RAM(B)の内容をRAM(A)へコピーする。

【S45】Churned-VP設定情報を受信した場合はステップS46へ、受信しない場合はステップS40へ戻る。

【S46】RAM(A)をバックアップ側、RAM(B)をアクティブ側と設定する。

【S47】Churned-VP設定情報を受信した場合は、RAM(A)へ上書きする。

【S48】Churning-Key更改タイミングで、RAM(A)をアクティブ側、RAM(B)をバックアップ側に設定する。

【S49】RAM(A)の内容をRAM(B)へコピーする。

【0103】次に復号化マスク手段14について説明する。ONU10ではo8状態になってからDechurnを行う。また、o8状態から他の状態に遷移して、再度o8状態になった時には、OLTとONU10のChurning-Keyが一致していないと、ユーザセルに対して誤ったDechurnを行ってしまう可能性がある。したがって、その間は復号化処理をマスクする必要がある。図13は復号化マスク処理を示す図である。

【S50】ONU10がo8状態から、その他の状態へ遷移する。

【S51】復号化マスク手段14は、o8状態からその他の状態へ遷移した時にマスクフラグをセットする。

【S52】復号化マスク手段14は、Dechurnのマスクを開始する(NotDechurn)。

【S53】その他の状態からo8状態へ遷移する。

【S54】復号化マスク手段14は、o8状態になってから、最初のChurning-Key更改タイミングを受信した場合に、マスクフラグをクリアして、Dechurnのマスク解除を行う。

【S55】新しいChurning-Keyと新しいChurned-VP設定情報にもとづいて、Dechurn

rnを行っていく。

【0104】このように、復号化マスク手段14は、o8状態に遷移してからChurning-Key更改タイミングとなるまでの期間は、復号化処理をマスクしてDechurnをかけず、ユーザセルはすべてNotChurnとする。

【0105】これにより、OLTとONU10のChurning-Keyの一致を確認して初めてDechurnを行うことができるので、セルの誤ったDechurnを防止することが可能になる。

【0106】次に本発明の変形例について説明する。図14はONU10の変形例を示す図である。なお、外部記憶制御手段13は、上述したので説明は省略する。暗号化設定情報記憶手段11aは、Churned-VP設定情報を記憶する記憶領域を1つだけ有している。

【0107】暗号化情報復号化処理手段12aは、フレーム構成を持つ情報ストリームを受信し、暗号化設定情報記憶手段11aで記憶しているChurned-VP設定情報を次フレームから有効にする。そして、Churned-VP設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う。

【0108】例えば、情報ストリーム中の1つのフレームの中で、VPI="001"（"001"はヘキサデータ）の情報が暗号化されている旨がChurned-VP設定情報に記載されているものとする。また、VPI="001"に対応するセルがセルC1だとする。

【0109】このような暗号化設定情報を1フレーム目にONU10aが受信した場合には、Churned-VP設定情報を暗号化設定情報記憶手段11aから読み出した後、次の2フレーム目からこのChurned-VP設定情報を有効にする。すなわち、2フレーム目からセルC1の復号化処理を行っていく。

【0110】このように、変形例であるONU10aでは記憶領域が1つだけでなく、また、Churning-Keyの更改時期と独立して、Churned-VP設定情報の有効タイミングを規定した。これにより、効率のよい復号化処理を行うことが可能になる。

【0111】次に本発明の光加入者線端局装置について説明する。図15は本発明の光加入者線端局装置の原理図である。光加入者線端局装置20は、ATM-PONのような光加入者系システムに接続し、暗号鍵を用いて、暗号化を行った情報部分を含む情報ストリームをONU10a~10n（総称してONU10）へ送信する。以降では、光加入者線端局装置20をOLT20と呼ぶ。

【0112】OLT20は、フラグ設定制御手段21と、暗号化設定情報送信制御手段22と、暗号化設定情報上書き手段23と、暗号化設定情報更改手段24から構成される。

【0113】フラグ設定制御手段21は、情報ストリー

ムの送信時にONU10の装置状態等にもとづいて、フラグを設定する。暗号化設定情報送信制御手段22は、設定されたフラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報（Churned-VP設定情報）の送信制御を行う。

【0114】暗号化設定情報上書き手段23は、Churned-VP設定情報をONU10へ再度送信する上書き処理を行う。暗号化設定情報更改手段24は、Churned-VP設定情報の更改タイミングを暗号化の更改周期終了時に一致させる。

【0115】次にフラグ設定制御手段21の初期暗号化（以下、初期Churn）フラグについて説明する。OLT20は、停止状態から運用状態（o8状態）へ遷移したONU10aに対し、Churned-VP設定情報を送信する。ONU10が停止状態からo8状態へ遷移した時に、Churned-VP設定情報を送信することを初期Churnと呼ぶ。

【0116】フラグ設定制御手段21では、初期Churnフラグを設けて、この初期Churnを実行する。初期Churnフラグの設定制御としては、ONU10が停止状態で初期Churnフラグをクリアし（0とし）、初期Churn完了で初期Churnフラグをセットする（1とする）。

【0117】暗号化設定情報送信制御手段22は、ONU10がo8状態へ遷移した時に、この初期Churnフラグをチェックし、初期Churnフラグがセットされていなければ、初期Churnを実行する。

【0118】図16は初期Churnフラグを用いた初期Churn処理手順を示すフローチャートである。なお、ONUには固有の番号nが与えられており、ONUの装置状態と後述する各種のフラグはnで管理される。

〔S60〕フラグ設定制御手段21は、ONU（n）が停止状態の場合に初期Churnフラグ（n）を0とする。

〔S61〕ONU（n）が停止状態からo8状態へ遷移する。

〔S62〕フラグ設定制御手段21は、o8状態に遷移したONU（n）が、初期Churnフラグ（n）が0であるか否かを判断する。0ならばステップS63へ行き、1ならば初期Churn完了とみなして終了する。

〔S63〕暗号化設定情報送信制御手段22は、初期Churnを実行する。ここで、初期Churnでは、ONU（n）に対して、4096VP分のChurned-VP設定情報を送信する。ONU（n）に対して、4096VP分のChurned-VP設定情報の送信が完了し、ONU（n）からメッセージ正常受信を通知するAckを、4096VP分受信すると初期Churnは完了となり、初期Churnフラグ（n）を1とする。

【0119】以上説明したように、初期Churnフラグを設けて、初期ChurnフラグをONU10が停止状態でクリア、初期Churnの完了時にセットすることにした。

【0120】これにより、ONU10が停止状態からo8状態へ遷移した時だけに初期Churnを実行することができ、他の状態から遷移した時には初期Churnを実行せず、無駄な処理を省くことが可能になる。

【0121】次にフラグ設定制御手段21の初期Churn実行中フラグについて説明する。初期Churnを行う場合には、初期Churn実行中フラグを設け、初期Churnの実行中はこの初期Churn実行中フラグをセットする。そして、初期Churn実行中フラグがセットされている場合は、次の初期Churn要求を受け付けずにすることにする。

【0122】すなわち、複数のONUが連続して停止状態からo8状態へ遷移した場合などに対し、最初に停止状態からo8状態へ遷移したONUに対して初期Churnを開始し、その時に初期Churn実行中フラグをセットして、その他のONUは待機させる。

【0123】そして、実行中のONUの初期Churnが完了すれば、待機しているONUの初期Churnを開始していく。図17は初期Churn実行中フラグを用いた初期Churn処理手順を示すフローチャートである。

【S70】フラグ設定制御手段21は、初期Churnフラグ(n)が0であることを確認する。

【S71】フラグ設定制御手段21は、初期Churn実行中フラグが0であるか否かを判断する。初期Churn実行中フラグが0であればステップS72へ、1であればステップS74へ行く。

【S72】フラグ設定制御手段21は、他のONUが初期Churn実行中ではないため、初期Churn実行中フラグを1とする。

【S73】暗号化設定情報送信制御手段22は、該当するONU(n)に対して初期Churnを行う。

【S74】暗号化設定情報送信制御手段22は、初期Churn実行中フラグが0になるまで（先行する初期Churnが終了するまで）、初期Churnを待機する。

【0124】以上説明したように、初期Churn実行中フラグが0である場合にのみ、対応するONUに対して初期Churnを行い、先行する初期Churnが終了した場合に、次のONUに対して初期Churnを行う構成とした。

【0125】これにより、複数のONUから連続で初期Churn要求が発生しても、初期ChurnをONU単位のシリアル処理として行うことができるので、複雑な輻輳処理をすることなく、効率よく初期Churnを行うことが可能になる。

【0126】次にフラグ設定制御手段21の設定更改失敗フラグについて説明する。初期Churnが完了したONUの運用中に、OLT20がChurned-VP設定情報の設定更改（設定変更）や上書き処理などを行った時に、ONU10へのChurned-VP設定情報の設定が失敗したとする。

【0127】このような、Churned-VP設定情報の設定更改失敗（LOA i (Churn)）が原因で状態落ち（停止状態へ遷移すること）が発生した場合は、再度、o8状態へ遷移した時に初期Churnを実行する必要がある。

【0128】そこで、フラグ設定制御手段21では、ONU10の運用中にChurned-VP設定情報の設定失敗の有無を示す設定更改失敗フラグを設ける。暗号化設定情報送信制御手段22は、設定更改失敗フラグがセットされている場合には、Churned-VP設定情報の設定更改に失敗したもののみならず、該当するONU10に対して初期Churnを実行する。

【0129】なお、以降の説明では、初期Churnが完了した運用中のONUに対して、Churned-VP設定情報の更改を行う場合の処理を、設定更改Churnと呼ぶ。

【0130】図18は設定更改失敗フラグを用いた初期Churn処理手順を示すフローチャートである。

【S80】フラグ設定制御手段21は、Churned-VP設定情報を送信した後、例えば、300ms以内にONU(n)からメッセージ正常受信を示すAckを受信しない場合、設定失敗とみなして、設定更改失敗フラグ(n)を1にする。

【S81】暗号化設定情報送信制御手段22は、ONU(n)に対する各種メッセージの送信を中断する。ONU(n)は停止状態となる。

【S82】暗号化設定情報送信制御手段22は、設定更改失敗フラグ(n)が1となっているONU(n)が、再度o8状態に遷移した時に、あらためて初期Churnを実行する。

【0131】以上説明したように、ONU10に対して設定更改Churnが失敗した場合には、設定更改失敗フラグを1として、再度初期Churnを行う構成とした。これにより、設定更改Churnの失敗時に、再度初期Churnを行って、Churned-VP設定情報を送信できるので、OLT20とONU10とのChurned-VP設定情報の設定不一致を防止することが可能になる。

【0132】次にフラグ設定制御手段21の設定更改未完了フラグについて説明する。初期Churnを完了したONU10が、設定更改Churn失敗以外の何らかの要因で状態落ちした場合には、Churned-VP設定情報の設定更改が終了していないことになる。そこで、フラグ設定制御手段21では、設定更改未完了フ

ラグを設け、終了していない場合は、設定更改未完了フラグをセットする。

【0133】そして、暗号化設定情報送信制御手段22は、該当するONUが再度o8状態へ遷移した時に、設定更改未完了フラグをチェックし、フラグがセットされれば初期Churnを実行する。

【0134】図19は設定更改未完了フラグを用いた初期Churn処理手順を示すフローチャートである。

【S90】ONU(n)が状態落ちた場合は、設定更改が未完了であることを示す設定更改未完了フラグ(n)を1とする。

【S91】暗号化設定情報送信制御手段22は、ONU(n)に対する各種メッセージの送信を中断する。ONU(n)は停止状態となる。

【S92】暗号化設定情報送信制御手段22は、設定更改未完了フラグ(n)が1となっているONU(n)が、再度o8状態に遷移した時に、あらためて初期Churnを実行する。

【0135】以上説明したように、ONU10の状態落ちが発生した場合には、設定更改未完了フラグを1として、再度初期Churnを行う構成とした。これにより、設定更改Churn失敗以外の場合でも、再度初期Churnを行って、Churned-VP設定情報を送信できるので、OLT20とONU10とのChurned-VP設定情報の設定不一致を防止することが可能になる。

【0136】次にフラグ設定制御手段21のChurn更改中フラグについて説明する。Churn更改周期の期間中に、設定更改Churn等(上書き処理も含め)を行うと、Churn更改と設定更改Churnが輻輳する可能性があり、設定更改Churnが正常に行われない場合がある。

【0137】したがって、フラグ設定制御手段21は、Churn更改フラグを設け、Churn更改周期中はこのフラグをセットする。Churn更改中フラグがセットしている期間(OLT20から送信されるメッセージの送信禁止期間となる)に、ONU10からChurned-VP設定情報の更改要求等があった場合は、要求をwaitさせ、Churn更改終了後に設定更改Churnを実行する。これにより、OLT20とONU10とのChurned-VP設定情報の設定不一致を防止することが可能になる。

【0138】次にフラグ設定制御手段21の設定更改要求フラグについて説明する。初期Churnが完了した運用中のONUに対し、OLT20が設定更改Churnを行う場合は、外部の保守端末装置よりONU単位に設定更改要求フラグをOLT20にセットする。

【0139】OLT20は、設定更改要求フラグがセットされたONUに対し、設定更改Churnを行う。設定更改Churn完了で設定更改要求フラグをクリアす

る。これにより、初期Churnで設定したChurned-VP設定情報をo8状態中に更改することが可能になる。

【0140】一方、設定更改要求フラグは、ONU単位とし、1回の設定更改で1ONUにつき1VPIの更改に制限する。このため、同報のVPIの設定更改の場合には、すべてのONUに対し同一設定ができる。

【0141】また、1ONUにつき1VPIと制限することで、1回の設定更改Churnは、Churn更改周期内で完了できるため、Churn設定更改処理時間を明確に規定できる。

【0142】次にフラグ設定制御手段21の設定更改実行中フラグについて説明する。設定更改Churnは、Churned-VP設定情報の設定更改処理であるため処理の優先順位が高い。そこで設定更改実行中フラグを設け、実行中はこのフラグをセットする。

【0143】設定更改実行中フラグのセット中は、他のONUからの要求をwaitさせることで割り込みを防止し、Churn設定更改の処理の優先順位を高くする。次に設定更改Churnの処理手順について図20～図23を用いて説明する。図20、図21は設定更改Churn開始時の処理手順を示すフローチャートである。

【S100】暗号化設定情報送信制御手段22は、設定更改要求フラグが1か否かを判断する(配下のONU10a～10nの1ONUでも設定更改要求があるか否かを判断する)。1ならばステップS101へ、0ならば終了する。

【S101】暗号化設定情報送信制御手段22は、SENDフラグ(フラグ設定制御手段21は、OLT20がChurned-VP設定情報を送信している場合は、SENDフラグをセットする)をチェックする。

【0144】SENDフラグが1であれば0になるまで待機し(ステップS101を繰り返す)、SENDフラグが0ならステップS102へ行く。

【S102】フラグ設定制御手段21は、SENDフラグをあらためて1にセットして、その他の要求を受け付けられないようにする。

【0145】ここで、ステップS103以降から並列処理となる。例えば、ONU10a、10b及び10cに対して設定更改要求があったものとする。ONU10a、10b及び10cの3つの並列処理が行われる。以降では、ONU10aに対する設定更改Churnの処理を説明する。

【S103】フラグ設定制御手段21は、設定更改要求フラグを0にする。

【S104】フラグ設定制御手段21は、設定更改実行中フラグを1にする。

【S105】暗号化設定情報送信制御手段22は、Churned-VP設定情報に更改VPIをセットし、C

hurned-VP設定情報の送信回数k（例えば、k=3）を設定する。

【S106】暗号化設定情報送信制御手段22は、Churn更改中フラグが1か否かを判断する。1の場合は0になるまで待機し（ステップS107を繰り返す）、0の場合はステップS107へ行く。

【S107】ONU10aが08状態から状態落ちしたか否かを判断する。すなわち、設定更改未完了フラグをチェックし、フラグが1ならばステップS110へ行き、フラグが0ならばステップS108へ行く。

【S108】暗号化設定情報送信制御手段22は、Churned-VP設定情報を送信し、Churned-VP設定情報を1回送信する度にkから1をデクリメント（k=k-1）し、送信回数を管理する。

【S109】k=0なら終了し、k≠0ならステップS106へ戻る。

【S110】暗号化設定情報送信制御手段22は、初期Churnを行う。

【0146】図22はACKメッセージの受信処理時のフローチャートを示す図である。OLT20がChurned-VP設定情報を送信した場合、ONU10aが正常にChurned-VP設定情報を受信すると、ACKメッセージをOLT20へ返送する。

【S120】暗号化設定情報送信制御手段22からChurned-VP設定情報の送信後（例えば、3回送信した後）、一定時間内（例えば、300ms以内）でACKメッセージの返答があるか計測する。タイムアウトした場合はステップS123へ、そうでなければステップS121へ行く。

【S121】Churn更改中フラグが1か否かを判断する。1の場合は0になるまで待機し（ステップS121を繰り返す）、0の場合はステップS122へ行く。

【S122】フラグ設定制御手段21は、設定更改実行中フラグを0にする。そして、有効となるChurned-VP設定情報を送信する。

【S123】フラグ設定制御手段21は、設定更改失敗フラグを1にする。

【S124】暗号化設定情報送信制御手段22は、初期Churnを行う。

【0147】図23は設定更改Churn終了時のフローチャートを示す図である。

【S130】すべてのONUの設定更改実行中フラグを監視し、設定更改実行中フラグがすべて0ならば、処理完了となりステップS131へ行く。そうでなければ0になるまで設定更改実行中フラグを監視し続ける（ステップS130を繰り返す）。

【S131】SENDフラグを0にして、他の処理に解放する。

【0148】次に暗号化設定情報上書き手段23について説明する。初期Churn完了後、Churned-

VP設定情報の設定更改がなければ、その後、OLT20がONU10に対してChurned-VP設定情報を送信することはない。

【0149】このため、従来では何らかの原因で、OLT20とONU10とのChurned-VP設定情報が設定不一致となった場合でも不一致となった状態を確認することができなかった。

【0150】そこで、本発明では暗号化設定情報上書き手段23を設け、ONU10が運用中、初期Churn完了をトリガとして、Churned-VP設定情報の上書き処理である上書きChurnを実行させることにした。これにより、何らかの原因でOLT20とONU10とのChurned-VP設定情報が設定不一致となった場合でも、上書きChurnで一致させることができる。

【0151】また、上書きChurnは、OLT20とONU10とのChurned-VP設定情報を一致させるための保護機能であるため、処理の優先順位は低く構わない。

【0152】そこで、上書きChurnのChurned-VP設定情報に対する送信要求は、他のメッセージ送信要求がある場合や設定更改Churnを行っている等の場合はwaitさせて、上書きChurnの優先順位を低くする。これにより、他のメッセージ送信を圧迫せずに、上書きChurnを実行できる。

【0153】さらに、暗号化設定情報上書き手段23の内部には、上書きChurnを実行するためのタイマが設けられる。このタイマは、上書きChurn用のChurned-VP設定情報の送信後に起動し、上書きChurnを行うべき最低限の周期を計測する。

【0154】そして、タイマで計測された次の送信時刻（他のメッセージ送信と競合しないように設定される）がくるまでは、上書きChurn用のChurned-VP設定情報は送信しない。

【0155】また、タイマの設定周期は、保守端末装置を通じて、任意の値を設定できる。したがって、上書きChurn設定に柔軟性を持たせることができる。次にChurning-Keyアップデートメッセージと、Churned-VP設定情報との送信時の競合防止について説明する。

【0156】ITU-T勧告G.983では、ONU10へのメッセージは、一定周期に発生する下りPLOAMセルにより送信される。したがって、PLOAMセル周期で送信すべきメッセージの調停処理を行って、ONU10へ送信するメッセージを決定しなければならない。

【0157】Churning-Keyアップデートメッセージは、図5で上述したように16×Tフレーム間隔で送信される。また、Churned-VP設定情報は、Churn更改中フラグがセットされていない間

で、3回の送信を完了する必要がある。

【0158】暗号化設定情報送信制御手段22は、Churning-Keyアップデートメッセージと、Churned-VP設定情報との調停処理を行った場合には、Churning-Keyアップデートメッセージを優先する。

【0159】すると、Churning-Keyアップデートメッセージは、16×Tフレーム間隔に自動的に送信される。その後、Churned-VP設定情報が例えば16×Tフレーム間隔で3回自動的に送信される。

【0160】すなわち、Churning-Keyアップデートメッセージと、Churned-VP設定情報の初回のみが調停対象となり、初回のChurning-Keyアップデートメッセージが送信されれば2回目、3回目のメッセージ送信は互いに競合を起こすことなく自動的に送信することが可能になる。

【0161】次に暗号化設定情報更改手段24について説明する。ITU-T勧告G.983では、Churning-Key更改タイミングは規定されているが、Churned-VP設定情報の更改タイミングは規定されていない。このため、OLT20ではChurned-VP設定情報に対して、不規則に設定情報の更改を行うと、OLT20とONU10とのChurned-VP設定情報の設定不一致を起こしてしまう可能性がある。

【0162】そこで、暗号化設定情報更改手段24は、Churning-Key更改タイミングでChurned-VP設定情報の更改を行うことにして不一致を防止する。

【0163】図24はChurned-VP設定情報の更改を示す図である。Churned-VP設定情報を3回送信完了後の最初のChurning-Key更改タイミングで、送信されたChurned-VP設定情報に対する設定更改を行っていく。

【0164】これにより、OLT20とONU10間でChurned-VP設定情報の設定更改を同期して行うことが可能になり、Churned-VP設定情報の設定不一致を防止することが可能になる。

【0165】

【発明の効果】以上説明したように、本発明の光加入者線終端装置は、現在使用中の暗号化設定情報を記憶するアクティブ側の第1の記憶手段と、新しく更改された暗号化設定情報を記憶するバックアップ側の第2の記憶手段との切り替え制御を行い、読み出した暗号化設定情報にもとづいて、次フレームの先頭から暗号化された情報部分の復号化処理を行う構成とした。これにより、暗号化設定情報の送信側と受信側との暗号化・復号化の処理タイミングのずれを防止し、高品質な通信制御を行うことが可能になる。

【0166】また、本発明の光加入者線終端装置は、受信装置へ情報ストリームを送信する際に、フラグの設定制御を行い、フラグにもとづいて、暗号化設定情報の送信制御を行う構成とした。これにより、暗号化設定情報の送信側と受信側との暗号化・復号化の処理タイミングのずれを防止し、高品質な通信制御を行うことが可能になる。

【図面の簡単な説明】

【図1】本発明の光加入者線終端装置の原理図である。

【図2】情報ストリームの構成及びChurned-VP設定情報のフォーマットを示す図である。

【図3】次フレームでDechurnを実現するためのブロック構成を示す図である。

【図4】次フレームからDechurnを行う際のタイミングチャートを示す図である。

【図5】Churning-Keyの更改シーケンスを示す図である。

【図6】2面RAMを持つONUのブロック構成を示す図である。

【図7】コピー動作手順を示すフローである。

【図8】コピー動作時のタイミングチャートを示す図である。

【図9】コピー中にChurned-VP設定情報を受信した際の動作を示すタイミングチャートである。

【図10】応答信号の返送制御手順を示すフローチャートである。

【図11】更改されたChurned-VP設定情報をSRAMから不揮発性メモリへ記憶させる場合の処理手順を示すフローチャートである。

【図12】暗号化設定情報記憶手段の電源復旧時の動作状態を示すフローチャートである。

【図13】復号化マスク処理を示す図である。

【図14】ONUの変形例を示す図である。

【図15】本発明の光加入者線終端装置の原理図である。

【図16】初期Churnフラグを用いた初期Churn処理手順を示すフローチャートである。

【図17】初期Churn実行中フラグを用いた初期Churn処理手順を示すフローチャートである。

【図18】設定更改失敗フラグを用いた初期Churn処理手順を示すフローチャートである。

【図19】設定更改未完了フラグを用いた初期Churn処理手順を示すフローチャートである。

【図20】設定更改Churn開始時の処理手順を示すフローチャートである。

【図21】設定更改Churn開始時の処理手順を示すフローチャートである。

【図22】ACKメッセージの受信処理時のフローチャートを示す図である。

【図23】設定更改Churn終了時のフローチャート

を示す図である。

【図24】 Churned-VP設定情報の更改を示す図である。

【図25】 ATM-PONシステムの構成を示す図である。

【符号の説明】

10 光加入者線終端装置

11 暗号化設定情報記憶手段

12 暗号化設定情報復号化処理手段

13 外部記憶制御手段

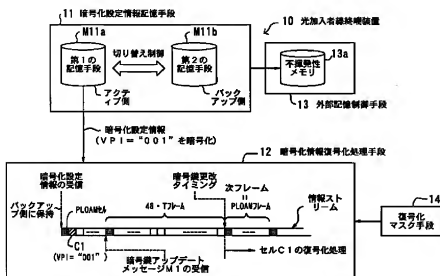
13a 不揮発性メモリ

14 復号化マスク手段

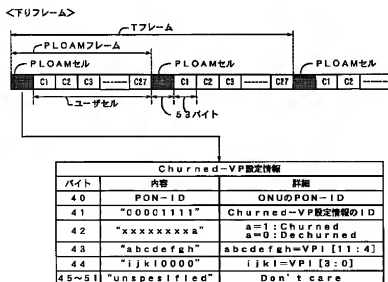
M11a 第1の記憶手段

M11b 第2の記憶手段

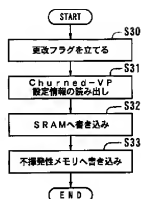
【図1】



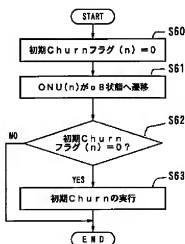
【図2】



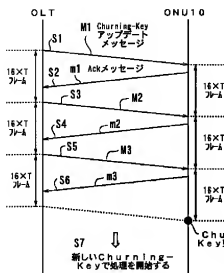
【図11】



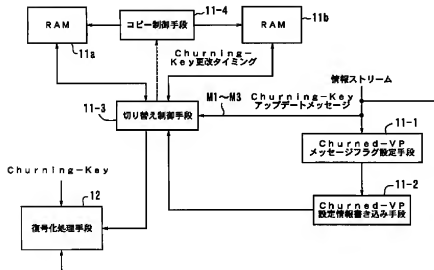
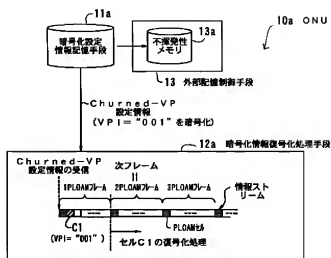
【図16】



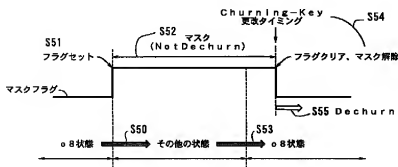
【図5】



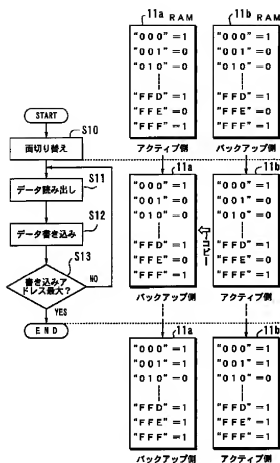
【図6】



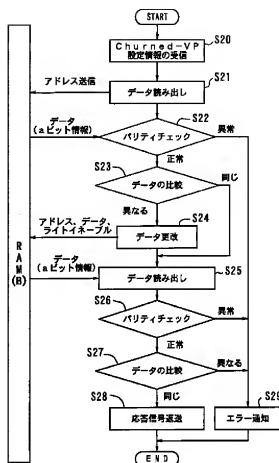
【図13】



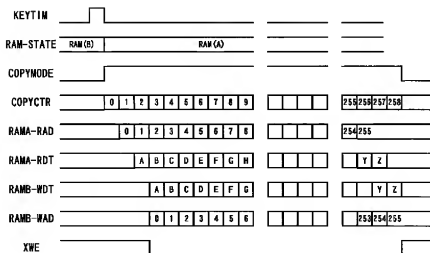
【図 7】



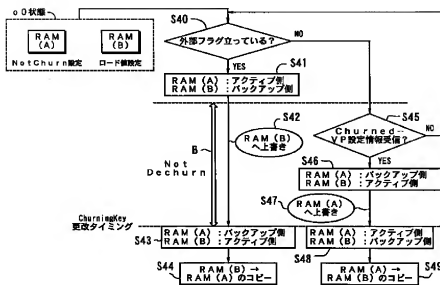
【図 10】



【図 8】

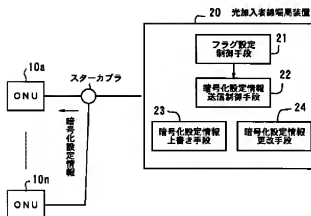


【図12】

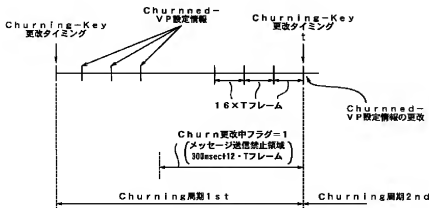
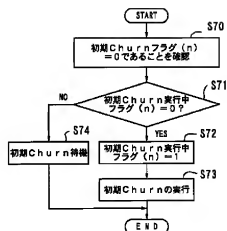


【図15】

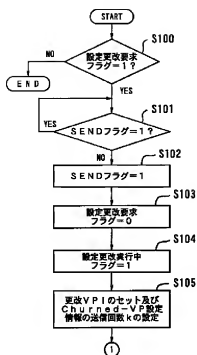
【図17】



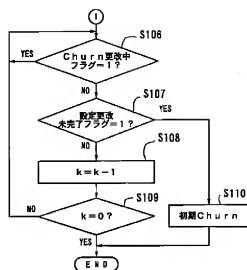
【図24】



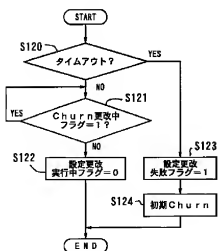
【図20】



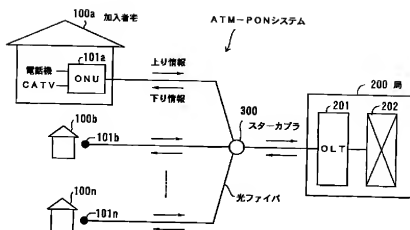
【図21】



【図22】



【図 25】



【手続補正書】

【提出日】平成12年2月7日（2000.2.7）

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】全文

【補正方法】変更

【補正内容】

【書類名】明細書

【発明の名称】光加入者線終端装置及び光加入者線端局装置

【特許請求の範囲】

【請求項1】 光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置において、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報に対し、現在使用中の暗号化設定情報を記憶するアクティブ側の第1の記憶手段と、新しく更改された暗号化設定情報を記憶するバックアップ側の第2の記憶手段とを含み、前記第1の記憶手段及び前記第2の記憶手段への記憶制御を行い、前記暗号鍵の暗号鍵更改タイミングで、前記第1の記憶手段と前記第2の記憶手段との切り替え制御を行う暗号化設定情報記憶手段と、フレーム構成を持つ前記情報ストリームを受信し、記憶している前記暗号化設定情報を、前記暗号鍵更改タイミング以後の次フレームから有効にして、前記暗号化設定情報が示す暗号化された前記情報部分に対する復号化処理を前記次フレームから行う暗号化情報復号化処理手段とを、

を有することを特徴とする光加入者線終端装置。

【請求項2】 前記暗号化設定情報記憶手段は、前記暗号鍵更改タイミングで前記第1の記憶手段と前記第2の

記憶手段とを切り替えた後、あらたにアクティブ側になった第1の記憶手段に記憶してある前記暗号化設定情報を、あらたにバックアップ側になった第2の記憶手段へコピーすることを特徴とする請求項1記載の光加入者線終端装置。

【請求項3】 前記暗号化設定情報記憶手段は、バックアップ側の第2の記憶手段へのコピー中に、あらたな暗号化設定情報を受信した場合は、前記コピーの終了後に前記あらたな暗号化設定情報を前記第2の記憶手段に記憶することを特徴とする請求項2記載の光加入者線終端装置。

【請求項4】 前記暗号化設定情報記憶手段は、読み出しポートが2つある前記第1の記憶手段及び前記第2の記憶手段を含むことを特徴とする請求項1記載の光加入者線終端装置。

【請求項5】 前記暗号化設定情報記憶手段は、前記暗号化設定情報を受信して、前記第1の記憶手段または前記第2の記憶手段へ正常に書き込めた否かを検証し、正常に書き込めた場合にのみ応答信号を返送することを特徴とする請求項1記載の光加入者線終端装置。

【請求項6】 前記暗号化設定情報を不揮発性メモリに記憶させる外部記憶制御手段をさらに有することを特徴とする請求項1記載の光加入者線終端装置。

【請求項7】 前記外部記憶制御手段は、受信した前記暗号化設定情報と、バックアップ側の前記第2の記憶手段に格納されている暗号化設定情報とを比較し、異なる暗号化設定情報のみ前記不揮発性メモリに記憶させることを特徴とする請求項6記載の光加入者線終端装置。

【請求項8】 前記外部記憶制御手段は、前記暗号化設定情報をメモリに記憶させ、電源断時に前記メモリから前記不揮発性メモリへ、一括して前記暗号化設定情報を

記憶させることを特徴とする請求項6記載の光加入者線終端装置。

【請求項9】 前記外部記憶制御手段は、前記暗号化設定情報をメモリに記憶させ、電源断時に前記メモリから前記不揮発性メモリへ、更改された暗号化設定情報のみ記憶させることを特徴とする請求項6記載の光加入者線終端装置。

【請求項10】 前記暗号化設定情報記憶手段は、電源復旧時の立ち上げ準備状態の期間のみ、前記不揮発性メモリからの前記暗号化設定情報を受け付けることを特徴とする請求項6記載の光加入者線終端装置。

【請求項11】 前記暗号化設定情報記憶手段は、電源復旧時に、前記不揮発性メモリから読み出された前記暗号化設定情報、またはあらたに送信された暗号化設定情報の一方を選択して有効にすることを特徴とする請求項6記載の光加入者線終端装置。

【請求項12】 前記暗号化情報の復号化処理を行える運用状態から、他の状態へ遷移して、再度前記運用状態になった場合は、前記運用状態になった時から前記暗号鍵更改タイミングを受信するまでの期間の復号化処理をマスクする復号化マスク手段を有することを特徴とする請求項1記載の光加入者線終端装置。

【請求項13】 光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置において、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報を記憶する暗号化設定情報記憶手段と、フレーム構成を持つ前記情報ストリームを受信し、記憶している前記暗号化設定情報を次フレームから有効にして、前記暗号化設定情報が示す暗号化された前記情報部分に対する復号化処理を前記次フレームから行う暗号化情報復号化処理手段と、

を有することを特徴とする光加入者線終端装置。

【請求項14】 光加入者系システムに接続して、暗号鍵を用いて暗号化を行った情報部分を含む情報ストリームを送信する光加入者線端局装置において、受信装置へ前記情報ストリームを送信する際に、フラグの設定制御を行うフラグ設定制御手段と、前記フラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報の送信制御を行う暗号化設定情報送信制御手段と、を有することを特徴とする光加入者線端局装置。

【請求項15】 前記フラグ設定制御手段は、初期暗号化フラグを有し、前記初期暗号化フラグを前記受信装置が停止状態でクリア、初期暗号化の完了時にセットすることを特徴とする請求項14記載の光加入者線端局装置。

【請求項16】 前記フラグ設定制御手段は、初期暗号化の実行中を示す初期暗号化実行中フラグを有すること

を特徴とする請求項14記載の光加入者線端局装置。

【請求項17】 前記フラグ設定制御手段は、前記受信装置に対する前記暗号化設定情報の設定更改が失敗と判断した場合は、設定更改失敗フラグをセットすることを特徴とする請求項14記載の光加入者線端局装置。

【請求項18】 前記フラグ設定制御手段は、前記受信装置が状態落ちたと判断した場合は、設定更改未完了フラグをセットすることを特徴とする請求項14記載の光加入者線端局装置。

【請求項19】 前記フラグ設定制御手段は、暗号化の更改周期中に暗号化更改中フラグをセットすることを特徴とする請求項14記載の光加入者線端局装置。

【請求項20】 前記フラグ設定制御手段は、前記暗号化設定情報の設定更改を行う際には、設定更改要求フラグをセットすることを特徴とする請求項14記載の光加入者線端局装置。

【請求項21】 前記フラグ設定制御手段は、1つの前記受信装置につき、1つの前記論理コネクションの更改に対して、前記設定更改要求フラグをセットすることを特徴とする請求項20記載の光加入者線端局装置。

【請求項22】 前記フラグ設定制御手段は、前記暗号化設定情報の設定更改実行中には、設定更改実行中フラグをセットすることを特徴とする請求項14記載の光加入者線端局装置。

【請求項23】 前記暗号化設定情報を前記受信装置へ再度送信する上書き処理を行う暗号化設定情報上書き手段をさらに有することを特徴とする請求項14記載の光加入者線端局装置。

【請求項24】 前記暗号化設定情報上書き手段は、優先度の高い他のメッセージの送信を行う場合は、前記上書き処理を待機させることを特徴とする請求項23記載の光加入者線端局装置。

【請求項25】 前記暗号化設定情報上書き手段は、前記暗号化設定情報の設定更改実行中は、前記上書き処理を待機させることを特徴とする請求項23記載の光加入者線端局装置。

【請求項26】 前記暗号化設定情報上書き手段は、タイマを有し、前記タイマに設定された周期にしたがって、前記上書き処理を行うことを特徴とする請求項23記載の光加入者線端局装置。

【請求項27】 前記タイマの周期は、外部から任意の値に設定されることを特徴とする請求項26記載の光加入者線端局装置。

【請求項28】 前記暗号化設定情報送信制御手段は、前記暗号化設定情報を複数回送信する場合に、1回目の前記暗号化設定情報の送信時のみ他メッセージと調停処理を行い、調停後は前記暗号化設定情報を一定間隔毎に自動的に送信することを特徴とする請求項14記載の光加入者線端局装置。

【請求項29】 前記暗号鍵の暗号鍵更改タイミング

で、前記暗号化設定情報の更改を開始する暗号化設定情報更改手段をさらに有することを特徴とする請求項14記載の光加入者線端局装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は光加入者線端局装置及び光加入者線端局装置に関し、特に光加入者系システムに接続して情報ストリームの受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線端局装置、及び光加入者系システムに接続して、暗号鍵を用いて暗号化を行った情報部分を含む情報ストリームを送信する光加入者線端局装置に関する。

【0002】

【従来の技術】近年、通信サービスの多様化は加速し、ビデオ・オン・デマンド、CATV、高速コンピュータ通信等の需要が拡大しつつある。このような大容量の通信サービスを低料金で提供するためには、加入者通信網を光化した光加入者系システムが不可欠である。

【0003】光加入者系システムとしては、1本の光ファイバを複数の加入者と共有するPDS (Passive Double Star) が提案されている。また、特に欧州を中心にしてPDS方式を採用したPON (Passive Optical Network) システムが注目されており、光ファイバを各家庭まで敷設するFTTH (Fiber To The Home) システムの実現に向けて開発が進んでいる。

【0004】また、このようなFTTHシステムの実現のためには、音声や動画などのリアルタイムの通信要求に対して、通信帯域や品質を保証するために、ATM (Asynchronous Transfer Mode) を利用したATM-PONの構築が、FSAN (Full Service Access Networks: 光通信事業を推進するために設立された国際的な通信業界団体) を中心に進められている。

【0005】図25はATM-PONシステムの構成を示す図である。加入者宅100a～100n内には、光バースト伝送を行うONU (Optical Network Unit: 光加入者線端局装置) 101a～101nが配置され、局200内にはOLT (Optical Line Terminal: 光加入者線端局装置) 201が配置される。

【0006】ONU101a～101nには電話機やCATV等が接続され、OLT201には交換機(ATM交換機、ISDN交換機等) 202が接続する。また、ONU101a～101nとOLT201は、スターカプラ300と接続する。

【0007】局200から加入者宅100a～100nへの下り情報(下りセル)は、1本の光ファイバから、スターカプラ300を介して、樹枝状に分岐された光ファイバを通じて送信される。また、加入者宅100a～100nから局200への上り情報(上りセル)は、樹枝状に分岐された光ファイバから、スターカプラ300を介して、1本に集約された光ファイバを通じて送信さ

れる。

【0008】このように、ATM-PONシステムは、スターカプラ300で局と複数の加入者との1:nで接続して構成する、ATMを使った光分岐型のアクセスネットワークである。

【0009】ここで、OLT201からONU101a～101nへの下り通信は、放送型であるため、ITU-T勧告G.983では、ONU毎の秘匿性を目的として、暗号化(Churning)方式が規定されている。

【0010】まず、OLT201は、下りメッセージにより、ONU(例えば、ONU101a)に暗号鍵を要求する。すると、応答したONU101aは、暗号鍵を生成し、OLT201に通知する。

【0011】OLT201は、その暗号鍵を使用して、ONU101aに対して送信すべき下り情報に対して暗号化を施す。この下り情報の暗号化はVP (Virtual Path: 仮想パス) 毎に行われる。

【0012】この場合、OLT201は、ONU101aに対し、VPI (Virtual Path Identifier: 仮想パス識別子) を単位として、どのVPに対して暗号化を施した(ON)か否か(OFF)を示す設定情報である暗号化設定情報を下りメッセージにより通知する。

【0013】このように、ATM-PONシステムの暗号化方式では、暗号鍵はONU毎に割り当てられ、下り情報の暗号化のON/OFFはVPI単位で行われる。そして、OLT201がONU101aに下りメッセージを用いて、暗号化設定情報を通知し、ONU101aでは自己の暗号鍵を用いて、暗号化されたVPの下り情報を復号化する。

【0014】

【発明が解決しようとする課題】しかし、上記のようなITU-T勧告G.983におけるATM-PONシステムの暗号化方式では、詳細な処理手順が規定されていない。

【0015】例えば、ONU101aでは、OLT201からの暗号化設定情報を保持しているが、ITU-T勧告G.983には復号化処理をいつ有効にすべきかが規定されていない。

【0016】したがって、OLT201側での暗号化処理、ONU101a側での復号化処理それぞれに時間的に大きなずれがあった場合などでは、暗号化・復号化が正常に行えないといった問題があった。

【0017】また、暗号化設定情報は、ONUの電源断時にはリセットされるため、電源復帰後は再度設定を行う必要があり、再立ち上げに時間がかかるなどといった問題もある。

【0018】このように、従来のATM-PONシステムの暗号化方式では、十分な技術が未だ確立されておらず、システム構築の実現のために高品質な通信制御を早

急に確立する必要がある。

【0019】本発明はこのような点に鑑みてなされたものであり、高品質な通信制御を確立し、情報の受信制御及び復号化処理を効率よく行う光加入者線終端装置を提供することを目的とする。

【0020】また、本発明の他の目的は、高品質な通信制御を確立し、情報の送信制御を効率よく行う光加入者線終端装置を提供することである。

【0021】

【課題を解決するための手段】本発明では上記課題を解決するために、図1に示すような、光加入者系システムに接続して情報ストリームを受信し、暗号鍵を用いて、暗号化された情報部分の復号化を行う光加入者線終端装置10において、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報に対し、現在使用中の暗号化設定情報を記憶するアクティブ側の第1の記憶手段M11aと、新しく更改された暗号化設定情報を記憶するバックアップ側の第2の記憶手段M11bを含み、第1の記憶手段M11a及び第2の記憶手段M11bへの記憶制御を行い、暗号鍵の暗号鍵更新タイミングで、第1の記憶手段M11aと第2の記憶手段M11bとの切り替え制御を行う暗号化設定情報記憶手段11と、フレーム構成を持つ情報ストリームを受信し、記憶している暗号化設定情報を、暗号鍵更新タイミング以後の次フレームから有効にして、暗号化設定情報で示す暗号化された情報部分に対する復号化処理を次フレームから行う暗号化情報復号化処理手段12と、を有することを特徴とする光加入者線終端装置10が提供される。

【0022】ここで、第1の記憶手段M11aは、現在使用中の暗号化設定情報を記憶する。第2の記憶手段M11bは、新しく更改された暗号化設定情報を記憶する。暗号化設定情報記憶手段11は、第1の記憶手段M11aと第2の記憶手段M11bを含み、第1の記憶手段M11a及び第2の記憶手段M11bへの記憶制御を行い、暗号鍵の暗号鍵更新タイミングで、第1の記憶手段M11aと第2の記憶手段M11bとの切り替え制御を行う。暗号化情報復号化処理手段12は、フレーム構成を持つ情報ストリームを受信し、記憶している暗号化設定情報を、暗号鍵更新タイミング以後の次フレームから有効にして、暗号化設定情報で示す暗号化された情報部分に対する復号化処理を次フレームから行う。

【0023】また、図15に示すような、光加入者系システムに接続して、暗号鍵を用いて暗号化を行った情報部分を含む情報ストリームを送信する光加入者線終端装置20において、受信装置へ情報ストリームを送信する際に、フラグの設定制御を行うフラグ設定制御手段21と、フラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報の送信制御を行う暗号化設定情報送信制御手段22と、を

有することを特徴とする光加入者線終端装置20が提供される。

【0024】ここで、フラグ設定制御手段21は、受信装置へ情報ストリームを送信する際に、フラグの設定制御を行う。暗号化設定情報送信制御手段22は、フラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報の送信制御を行う。

【0025】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図1は本発明の光加入者線終端装置の原理図である。光加入者線終端装置10は、ONUに該当し、ATM-PON等の光加入者系システムに接続してOLTから送信される情報ストリーム（複数のセルで構成される）を受信する。

【0026】そして、自己の装置で生成した暗号鍵を用いて、情報ストリーム内の暗号化された情報部分に対して復号化を行う。以降では、光加入者線終端装置10をONU10と呼ぶ。

【0027】暗号化設定情報記憶手段11は、暗号化設定情報を記憶するために、第1の記憶手段M11aと第2の記憶手段M11bの2面の記憶領域を有している。ここで、暗号化設定情報とは、論理コネクション毎に暗号化を施したか否かを示す設定情報である。具体的には、VPIを単位として、どのVPIに対して暗号化を施したか否かを示す設定情報のことをいう。

【0028】第1の記憶手段M11aは、アクティブ側であり、現在使用中（読み出し中）の暗号化設定情報を記憶している。第2の記憶手段M11bは、バックアップ側であり、新しく更改された暗号化設定情報を記憶する。

【0029】そして、暗号化設定情報記憶手段11は、第1の記憶手段M11aと第2の記憶手段M11bへの記憶制御（書き込み制御）を行い、暗号鍵の暗号鍵更新タイミング（古い暗号鍵を新しい暗号鍵に更改した時のタイミング）で、第1の記憶手段M11aと第2の記憶手段M11bとの切り替え制御を行う。詳細は後述する。

【0030】暗号化情報復号化処理手段12は、フレーム構成を持つ情報ストリームを受信し、記憶している暗号化設定情報を第1の記憶手段M11aから読み出して、暗号鍵更新タイミング以後の次フレームから、読み出した暗号化設定情報を有効にする。そして、暗号化設定情報で示す暗号化された情報部分に対する復号化処理を次フレームから行う。

【0031】例えば、情報ストリーム中の1つのフレームの中で、VPI＝“001”（“001”はヘキサデータ）の情報が暗号化されている旨が暗号化設定情報に記載されているものとする。また、VPI＝“001”に対応するセルがセルC1だとする。

【0032】図に示すように、暗号化設定情報を受信すると、バックアップ側の第2の記憶手段M11bに記憶する。その後、暗号鍵アップデータメッセージM1を受信して、48×Tフレーム経過した後の暗号鍵更改タイミング以後の次フレームからこの暗号化設定情報を有効にする。このようにして復号化処理の有効タイミングを明確に規定したので、暗号化処理、復号化処理の不一致を防止することが可能になる。なお、詳細動作は後述する。

【0033】外部記憶制御手段13は、暗号化設定情報を書き換えメモリ13aに記憶させる。復号化マスク手段14は、暗号化情報の復号化を行える運用状態から、他の状態へ遷移して再度運用状態になった場合に、運用状態になった時から暗号鍵更改タイミングを受信するまでの期間の復号化処理をマスクする。なお、外部記憶制御手段13及び復号化マスク手段14の詳細については後述する。

【0034】次に本発明のONU10の具体的な構成・動作について詳しく説明する。なお、以降では暗号化処理をChurn、復号化処理をDechurn、暗号化設定情報をChurned-VP設定情報と呼ぶ。

【0035】図2は情報ストリームの構成及びChurned-VP設定情報のフォーマットを示す図である。OLTから送信される情報ストリームの1つのフレーム（PLOAMフレーム）は、OLTとONU10間で制御情報を通信するためのPLOAM（Physical Layer Operation And Management）セルと、実際の通信情報であるユーザセルC1～C27から構成される。そして、このPLOAMフレーム2つで、Tフレームと呼ぶ（伝送レートが150Mbpsモードの場合）。

【0036】また、PLOAMセル及びユーザセル共に、1セルが53バイトである。Churned-VP設定情報は、PLOAMセルで送信される各種制御情報のうちの1つであり、PLOAMセルの40バイト～51バイトまでがChurned-VP設定情報として定義されている。

【0037】40バイト目は、PON-IDであり、ONU10の識別子としてPON-IDが記される。41バイト目は、Churned-VP設定情報であることを知らせる識別子が記される。この識別子は“00001111”（左側がMSB、右側がLSBである。以降同様）である。

【0038】43、44バイト目は、VPIを示す情報であり、43、44バイト目に記されるVPI情報をVPI[11:0]と表す。また、43バイト目の“abcdefgh”をVPI[11:4]と表し、44バイト目の“ijkl”をVPI[3:0]と表す。なお、ATM-PONシステムVPIの値は4096個ある（4096VPある）。また、ユーザセルも、どのVPから流れてきたものかを示すために、同様のVPI情報

をそれぞれ個別に有している。

【0039】ここで、[M:N]は、下位Nビットから上位Mビットの（M-N+1）ビットのデータであることを意味する。42バイト目は、43、44バイト目に記されたVPIに対して、Churnされているか否かを示す情報が記される。内容は“xxxxxxxx”（x=未定義）であり、a（アクトビット）=1ならChurnされており（したがって、ONU10ではDechurnしなければならない）、a=0ならChurnされていない。45～51バイト目は未定である。

【0040】次に暗号鍵更改について説明する。本発明のONU10が適用されるATM-PONシステムでは、OLT側に位置する保守端末装置からの要求毎に、暗号鍵（以降、Churning-Keyと呼ぶ）の更改（鍵を新しくすること）を行っている。図3はChurning-Keyの更改シーケンスを示す図である。

【S1】OLTは、新しいChurning-Keyの送信要求として、Churning-KeyアップデータメッセージM1をONU10に送信する。

【S2】ONU10は、新しいChurning-Keyを生成して、ACKメッセージm1に乗せてOLTに返送する。

【S3】OLTは、Churning-KeyアップデータメッセージM1を送信してから16×Tフレーム経過した後、Churning-KeyアップデータメッセージM2をONU10に送信する。

【S4】ONU10は、ステップS2と同様に、ACKメッセージm2に更改したChurning-Keyの情報を乗せてOLTに返送する。

【S5】OLTは、Churning-KeyアップデータメッセージM2を送信してから16×Tフレーム経過した後、Churning-KeyアップデータメッセージM3をONU10に送信する。

【S6】ONU10は、ステップS2及びステップS4と同様に、ACKメッセージm3をOLTに返送する。

【S7】OLTがChurning-KeyアップデータメッセージM1をONU10へ送信してから48×Tフレーム経過した時点（Churning-Key更改タイミング）で、新しいChurning-Keyが使用される。すなわち、OLTはこの新しいChurning-KeyでChurnを行い、ONU10は新しいChurning-KeyでDechurnを行う。なお、16×Tフレームのカウントは、図に示すようにOLT、ONU10の双方で行う。

【0041】したがって、OLTがChurning-KeyアップデータメッセージM1をONU10に送信してから、48×Tフレーム経過するまでは、旧タイプのChurning-Keyを用いて、OLTとONU10間でChurn/Dechurnが行われる。

【0042】次に暗号化設定情報記憶手段11の2面R

AM構成及びコピー動作について説明する。図3で説明したように、Churning-KeyをChurning-Key更改タイミングで更改した場合には、Churned-VP設定情報もこのタイミングでONU10側で更改しなければならない。したがって、Churning-Key更改タイミングとなる以前にOLTから送信された新しいChurned-VP設定情報を記憶しておく必要がある。

【0043】図4は2面RAMを持つONU10のブロック構成を示す図である。Churned-VPメッセージフラグ設定手段11-1とChurned-VP設定情報書き込み手段11-2は暗号化設定情報記憶手段11内に含まれ、復号化処理手段12は暗号化情報復号化処理手段12に対応する。

【0044】Churned-VPメッセージフラグ設定手段11-1は、PLOAMセルのChurned-VP設定情報を受信した場合に、Churned-VPメッセージフラグをセットする。

【0045】Churned-VP設定情報書き込み手段11-2は、Churned-VPメッセージフラグをライトイネーブルの1つとして用い、RAM M11a、M11b（暗号化設定情報記憶手段11を含む記憶手段に対応する）にChurned-VP設定情報の書き込みを行う。RAM M11a、M11bは、256アドレスであり、1アドレスが格納するデータ領域は16ビットある。また、切り替え制御手段11-3とコピー制御手段11-4は暗号化設定情報記憶手段11内に含まれる。

【0046】最初、RAM M11aを、アクティブ側（RAM M11aのアドレスをVPI {11:4}）として、現在Churned-VP設定情報が読み出されているRAM）とし、RAM M11bをバックアップ側（OLTから送信された新しいChurned-VP設定情報を次のChurning-Key更改タイミングまで保持しておくRAM）とする。

【0047】切り替え制御手段11-3は、Churning-KeyアップデータメッセージM1～M3を3回受信して、Churning-KeyアップデータメッセージM1から48×Tフレーム経過した場合には、その時間をChurning-Key更改タイミングとして認識する。

【0048】そして、Churning-Key更改タイミングでRAM M11aとRAM M11bを切り替えて、RAM M11bをアクティブ側、RAM M11aをバックアップ側とする。

【0049】一方、このままでは古いChurned-VP設定情報を記憶しているRAM M11aがバックアップ側になってしまう。したがって、コピー制御手段11-4は、新しくアクティブ側になったRAM M11bからデータをRAM M11aへコピーしていく。

【0050】なお、RAM M11a及びRAM M11bは共に読み出しポートを2つ有している。このため、例えば、アクティブ側のRAMからバックアップ側のRAMへコピーが行われている最中でも、アクティブ側RAMからChurned-VP設定情報を読み出すことができる。

【0051】図5はコピー動作手順を示すフローである。なお、最初はRAM M11aをアクティブ側、RAM M11bをバックアップ側とし、RAM M11aとRAM M11bのそれぞれは、図に示すような値（例えば、“000”=1とは、VPI=“000”のaビット情報が1ということ）が格納されているものとする。

【S10】切り替え制御手段11-3は、Churning-Key更改タイミングでRAM M11aとRAM M11bを切り替える。

【S11】コピー制御手段11-4は、切り替え制御手段11-3から通知されたChurning-Key更改タイミングを受信するで、RAM M11bに対する読み出しアドレスをインクリメントして、RAM M11bからデータを読み出す。

【S12】コピー制御手段11-4は、RAM M11aに対する書き込みアドレスをインクリメントして、RAM M11bから読み出したデータをRAM M11aへ書き込んでいく。

【S13】コピー制御手段11-4は、書き込みアドレスが最大になったか否かを判断する。最大でなければステップS11へ戻って、ステップS11、S12を繰り返していき、最大であればコピーを終了する。

【0052】図6はコピー動作時のタイミングチャートを示す図である。KEYTIMは、Churning-Key更改タイミングパルスである。RAM-STATEは、2面のRAMがアクティブ側かバックアップ側かを示す信号であり、図では更改前のRAMステートとしてRAM (B) がアクティブ側であり、更改後にRAM (A) がアクティブ側となるものとする。

【0053】COPYMODEは、コピー動作時に“H”となる信号である。COPYCTRは、COPYMODEが“H”の間、RAMの256アドレス数をカウントするための信号である。実際には、XWEが図に示すような位相となるので、259進カウンタを用いている。

【0054】RAMA-RADは、新しくアクティブ側になったRAM (A) の読み出しアドレスを示す信号であり、COPYCTRを1段ずらした信号を読み出しアドレスとして使用する。

【0055】RAMA-RDTは、RAMA-RADのアドレスで読み出された読み出しデータを示す信号であり、アドレス0に対して読み出しデータA、アドレス1に対して読み出しデータB、……である。RAMA-R

ADから1段ずれた位置に読み出しデータが出力される。

【0056】RAMB-WDTは、バックアップ側となったRAM(B)への書き込みデータを示す信号であり、RAMA-RDTを1段ずらした信号を書き込みデータとして使用する。

【0057】RAMB-WADは、RAMB-WDTをRAM(B)へ書き込むための書き込みアドレスを示す信号である。アドレス0に対して書き込みデータA、アドレス1に対して書き込みデータB、……をRAM(B)へ書き込んでいく(コピーする)。

【0058】XWEは、バックアップ側となったRAM(B)へ、RAM(A)の内容をコピーする場合の書き込みアドレス信号であり、アクティブ“L”である。以上説明したように、本発明では、2面あるRAMの切り替えを行った場合に、新しいChurned-VP設定情報を受け、切り替え後にバックアップ側となったRAMへコピーする構成にした。

【0059】これにより、バックアップ側も新しいChurned-VP設定情報を受け持つことができ、OLT側とのChurned-VP設定情報の不一致を防止することが可能になる。

【0060】次にコピー中にあらたなChurned-VP設定情報を受信した場合の動作について説明する。Churning-Key更改タイミングは、PLOAM周期を最小単位として、フレーム数を数えているので必ずPLOAMセルの位置で上がることになる。

【0061】この場合、Churning-Key更改タイミングの位置のPLOAMセルがChurned-VP設定情報を持つセルの場合、バックアップ側のRAMへは、アクティブ側のRAMのデータのコピーが開始されているため、その情報をバックアップ側のRAMへ即時に書き込むことができない。

【0062】そこで、コピー中にこのようなChurned-VP設定情報を受信した場合には、フラグ(上述したCOPYMODEをフラグとして利用)をセットし、コピー終了後にフラグをクリアして、バックアップ側のRAMへ上書きする構成とする。

【0063】図7はコピー中にChurned-VP設定情報を受信した際の動作を示すタイミングチャートである。COPYMODEは、コピー動作時に“H”となる信号である。CHURNED-TRは、Churned-VP設定情報を受信したことを示すトリガ信号であり、受信時に“H”となる。

【0064】CHURNED-LTは、COPYMODEが“H”で、CHURNED-TRが“H”になった場合にCHURNED-TRをラッチした信号である。CVP-CTRは、CHURNED-LTの立ち下がりによってロードされて、バックアップ側のRAMへ書き込むための書き込みアドレスを示す信号である。

【0065】以上説明したように、コピー中に受信したChurned-VP設定情報に対しては、コピー終了後に書き込む構成とした。このように、コピーを優先して、その後に上書きすることが可能になる。

【0066】次にChurned-VP設定情報を受信した際の応答信号の返送制御について説明する。ITU-T勧告G.983では、ONU10がChurned-VP設定情報を受信した場合、受信したことをOLTへ通知するための応答信号を返送する旨が規定されているが、返送条件については規定されていない。

【0067】したがって、本発明の暗号化設定情報記憶手段11は、Churned-VP設定情報を受信してRAMへ書き込んだ際に、再度読み出してバリファイチェック(書き込んだ値と読み出した値とを比較する)を行う。そして、正常に書き込んだ場合にのみ、ONU10はOLTへ応答信号を返送する。

【0068】図8は応答信号の返送制御手順を示すフローチャートである。RAM(A)をアクティブ側、RAM(B)をバックアップ側とし、コピー動作は終了しているものとする。

【0069】したがって、Churned-VP設定情報を受信した際には、RAM(B)へ書き込み、再度RAM(B)から読み出してバリファイチェックを行った後に応答信号の返送制御を行う。

【S20】Churned-VP設定情報を受信する。
【S21】Churned-VP設定情報に対するアドレスのデータをRAM(B)から読み出す。すなわち、VPI[11:4]のアドレスに対応するデータのVPI[3:0]の位置にあるデータ(aビット情報)をRAM(B)から読み出す。

【S22】RAM(B)から読み出したデータのバリファイチェック(LS1間同士のデータ伝送などでは、データ送受信の信頼性確保のため、誤り訂正を行う必要があり、誤り訂正符号をデータに付加して送受信を行っている)を行う。正常の場合はステップS23へ行く。バリファイエラーの場合はステップS29へ行く。

【S23】RAM(B)から読み出したデータと、受信したChurned-VP設定情報のaビット情報とを比較する。値が異なる場合はステップS24へ行き、値が同じ場合はステップS25へ行く。

【S24】ステップS21と同じアドレスへ、更改されたaビット情報を書き込む。

【S25】ステップS21と同じアドレスからデータを再び読み出す。

【S26】RAM(B)から読み出したデータのバリファイチェックを行う。正常ならばステップS27へ行く。バリファイエラーの場合はステップS29へ行く。

【S27】RAM(B)から読み出したデータと、受信したChurned-VP設定情報のaビット情報とを

比較する。値が同じ場合はステップS28へ行き、値が異なる場合はステップS29へ行く。

【S28】RAM (B)へ正常に書き込んだので、Churned-VP設定情報を受信したことを通知するための応答信号をOLTへ返送する。

【S29】ONU10の全体制御を行っている全体制御部へエラー通知を送信する。

【0070】以上説明したように、本発明の暗号化設定情報記憶手段11は、Churned-VP設定情報を受信し、RAMへ書き込んだ際に正常に書き込んだ否かを検証する。そして、ONU10は、正常に書き込んだ場合にのみ応答信号を返送する構成とした。これにより、OLT側とのChurned-VP設定情報の設定不一致を防止することが可能になる。

【0071】次に外部記憶制御手段13について説明する。本発明のONU10ではバックアップ電源を有しており、外部記憶制御手段13は、電源断時にはバックアップ電源を利用して、Churned-VP設定情報を不揮発性メモリ（フラッシュメモリなど）13aに記憶させる。

【0072】これにより、電源断になっても不揮発性メモリ13aにChurned-VP設定情報を保持することができるので、電源復旧後に再度Churned-VP設定情報をOLTから送信要求しなくてもよい。

【0073】また、外部記憶制御手段13は、一旦、不揮発性メモリ13aにChurned-VP設定情報を格納した後は、あらたに受信したChurned-VP設定情報と、バックアップ側のRAMに格納されているChurned-VP設定情報とを比較し、異なるChurned-VP設定情報のみを不揮発性メモリ13aに記憶させる。

【0074】具体的には、図8のステップS24で、更改されたaビット情報を書き込んだ際に、aビット情報が更改されていることを示す更改フラグを暗号化設定情報記憶手段11がセットする。

【0075】外部記憶制御手段13は、この更改フラグが立っている場合に、バックアップ側のRAMから、対応するアドレスのデータを読み出し、不揮発性メモリ13aへ記憶させる。このように、更改されたChurned-VP設定情報だけを記憶していくので効率よく不揮発性メモリ13aに記憶させることができる。

【0076】一方、不揮発性メモリ13aには書き込み回数が制限されているものが多いので、さらに書き込み回数を削減する工夫が必要である。したがって、外部記憶制御手段13では、電源復旧時にはChurned-VP設定情報を例えばSRAM (Static-RAM) 等のメモリに一旦記憶させ、電源断時にはSRAMから不揮発性メモリ13aへ、一括してChurned-VP設定情報記憶させてもよい。これにより、不揮発性メモリ13aへのアクセス回数を削減することが可能になる。

【0077】また、一旦不揮発性メモリ13aからSRAMへ一括書き込みを行った初期動作以降は、更改フラグが立っているChurned-VP設定情報のみをSRAMへ書き込む。そして、電源断時にはSRAMから不揮発性メモリ13aへ、更改されたChurned-VP設定情報のみを記憶させてもよい。

【0078】図9は更改されたChurned-VP設定情報をSRAMから不揮発性メモリ13aへ記憶させる場合の処理手順を示すフローチャートである。

【S30】暗号化設定情報記憶手段11は、Churned-VP設定情報が更改されている場合は、更改フラグを立てる。

【S31】外部記憶制御手段13は、バックアップ側のRAMから、更改フラグにもとづいて対応するChurned-VP設定情報を読み出す。

【S32】外部記憶制御手段13は、更改されたChurned-VP設定情報をSRAMへ書き込む。

【S33】外部記憶制御手段13は、ONU10の電源断時に、SRAMが格納している情報を不揮発性メモリ13aへ書き込む。

【0079】電源断時には、更改されたChurned-VP設定情報のみをSRAMから不揮発性メモリ13aへ記憶させてもよい。これにより、不揮発性メモリ13aへのアクセス回数をさらに削減することが可能になる。

【0080】次に電源復旧時のONU10の動作について説明する。ITU-T勧告G. 983では、ONUの動作状態としてO1状態～O10状態を定めており、特にONUの電源復旧後の状態は、O1状態またはO9状態であることが規定されている。

【0081】O1状態とは、ONUの電源復旧後の初期状態のことである。O9状態とは、緊急停止状態であり、この状態になると、ONUはネットワークから切り離されて、通信ができなくなる。

【0082】また、本発明では、ONU10の電源復旧後の動作状態として、O1状態へ遷移させるべきか、またはO9状態へ遷移させるべきかを判断するための立ち上げ準備状態（以降、O0状態と呼ぶ）をあらたに設けることにした。

【0083】本発明の暗号化設定情報記憶手段11では、このO0状態を利用して、電源復旧時のO0状態の期間のみに、不揮発性メモリ13aからChurned-VP設定情報を受け付けることにする。

【0084】これにより、ONU10の運用状態（以降、O8状態と呼ぶ）中に、誤ってRAMに対する外部からの書き込みがあった場合でもその情報を有効としないので、OLT側とのChurned-VP設定情報の不一致を防止することが可能になる。

【0085】一方、暗号化設定情報記憶手段11は、O0状態の時に、不揮発性メモリ13aから読み出された

Churned-VP設定情報と、あらたに送信された暗号化設定情報とのいずれを有効にすべきか判断して選択することができる。

【0086】すなわち、ONU10は、0状態時に不揮発性メモリ13aから再ロードしたChurned-VP設定情報を有効にするかどうかは未定とする。なぜなら、OLTから送信される、あらたなChurned-VP設定情報をONU10へ設定したい（有効とした）場合があるからである。そこで、2面あるRAMのうち、一方を不揮発性メモリ13aからロードした値を持っておくRAM、他方をNotChurnにするためにイニシャライズ（以降、NotChurn設定と呼ぶ）をかけたRAMを0状態時に設定しておく。

【0087】そして、不揮発性メモリ13aからロードした値を有効にしたい場合は、外部フラグをセットし、そのロードした値をRAMに保持させ、その後、受信したChurned-VP設定情報をこのRAMに上書きしていく。

【0088】また、外部フラグがセットされていない場合は、OLTからのChurned-VP設定情報を、NotChurn設定されたRAMへ書き込んでいく。それぞれの場合ともChurning-Key更改タイミングで、コピー動作が開始される。

【0089】図10は暗号化設定情報記憶手段11の電源復帰時の動作状態を示すフローチャートである。RAM(A)をNotChurn設定されたRAMとし、RAM(B)を不揮発性メモリ13aからロードされたChurned-VP設定情報を保持するロード値設定RAMとする。なお、期間BではユーザセルはNotDechurnである。

【S40】外部フラグがセットされているか否かを判断する。セットしていればステップS41へ、セットしていなければステップS45へ行く。

【S41】RAM(A)をアクティブ側、RAM(B)をバックアップ側と設定する。

【S42】Churned-VP設定情報を受信した場合は、RAM(B)へ上書きする。

【S43】Churning-Key更改タイミングで、RAM(A)をバックアップ側、RAM(B)をアクティブ側と設定する。

【S44】RAM(B)の内容をRAM(A)へコピーする。

【S45】Churned-VP設定情報を受信した場合はステップS46へ、受信しない場合はステップS40へ戻る。

【S46】RAM(A)をバックアップ側、RAM(B)をアクティブ側と設定する。

【S47】Churned-VP設定情報を受信した場合は、RAM(A)へ上書きする。

【S48】Churning-Key更改タイミング

で、RAM(A)をアクティブ側、RAM(B)をバックアップ側と設定する。

【S49】RAM(A)の内容をRAM(B)へコピーする。

【0090】次に復号化マスク手段14について説明する。ONU10では08状態になってからDechurnを行う。また、08状態から他の状態に移移して、再度08状態になった時には、OLTとONU10のChurning-Keyが一致していないと、ユーザセルに対して誤ったDechurnを行ってしまう可能性がある。したがって、その間は復号化処理をマスクする必要がある。図11は復号化マスク処理を示す図である。

【S50】ONU10が08状態から、その他の状態へ遷移する。

【S51】復号化マスク手段14は、08状態からその他の状態へ遷移した時にマスクフラグをセットする。

【S52】復号化マスク手段14は、Dechurnのマスクを開始する(NotDechurn)。

【S53】その他の状態から08状態へ遷移する。

【S54】復号化マスク手段14は、08状態になってから、最初のChurning-Key更改タイミングを受信した場合に、マスクフラグをクリアして、Dechurnのマスク解除を行う。

【S55】新しいChurning-Keyと新しいChurned-VP設定情報にもとづいて、Dechurnを行うしていく。

【0091】このように、復号化マスク手段14は、08状態に移移してからChurning-Key更改タイミングとなるまでの期間は、復号化処理をマスクしてDechurnをかけず、ユーザセルはすべてNotChurnとする。

【0092】これにより、OLTとONU10のChurning-Keyの一致を確認して初めてDechurnを行うことができるので、セルの誤ったDechurnを防止することが可能になる。

【0093】次に本発明の変形例について説明する。図12はONU10の変形例を示す図である。なお、外部記憶制御手段13は、上述したので説明は省略する。暗号化設定情報記憶手段11aは、Churned-VP設定情報を記憶する記憶領域を1つだけ有している。

【0094】暗号化情報復号化処理手段12aは、フレーム構成を持つ情報ストリームを受信し、暗号化設定情報記憶手段11aで記憶しているChurned-VP設定情報を次フレームから有効にする。そして、Churned-VP設定情報が示す暗号化された情報部分に対する復号化処理を次フレームから行う。

【0095】例えば、情報ストリーム中の1つのフレームの中で、VPI="001"（"001"はヘキサデータの）情報が暗号化されている旨がChurned-VP設定情報に記載されているものとする。また、VP

I = “001”に対応するセルがセルC1だとする。

【0096】このような暗号化設定情報を1フレーム目にONU10aが受信した場合には、Churned-VP設定情報を暗号化設定情報記憶手段11aから読み出した後、次の2フレーム目からこのChurned-VP設定情報を有効にする。すなわち、2フレーム目からセルC1の復号化処理を行っていく。

【0097】このように、変形例であるONU10aでは記憶領域が1つだけでよく、また、Churning-Keyの更改時期と独立して、Churned-VP設定情報の有効タイミングを規定した。これにより、効率のよい復号化処理を行うことが可能になる。

【0098】図13は次フレームでDechurnを実現するためのブロック構成を示す図である。なお、Churned-VPメッセージフラグ設定手段11-1とChurned-VP設定情報書き込み手段11-2は暗号化設定情報記憶手段11内に含まれ、復号化処理手段12は暗号化情報復号化処理手段12に対応する。

【0099】Churned-VPメッセージフラグ設定手段11-1は、PLOAMセルのChurned-VP設定情報を受信した場合に、Churned-VPメッセージフラグをセットする。

【0100】Churned-VP設定情報書き込み手段11-2は、Churned-VPメッセージフラグをライトイネーブルの1つとして用い、RAM11a（暗号化設定情報記憶手段11aを含む記憶手段に対応する）にChurned-VP設定情報の書き込みを行う。RAM11aは、256アドレスであり、1アドレスが格納するデータ領域は16ビットある。

【0101】書き込み処理としては、VPI [11:0]のうち、VPI [11:4]の8ビットをRAM11aへの書き込みアドレスとし、aビット情報をRAM11aへの書き込みデータとする。

【0102】ここで、VPI [11:4]をRAM11aのアドレスとした場合に、この1つのアドレスに16ビットの格納領域があるため、1アドレスにVPI [3:0]（4ビット）の16通りのVPI値を割り当てることができる。

【0103】すなわち、RAMの1つのアドレスに対して、16通りのVPIを設定でき、この16通りのVPIに対応するaビット情報を、RAM11aの格納領域である16ビットの各ビットに対してデータとして書き込んでいく。したがって、RAM11aは、4096個のaビット情報の記憶領域を有することになる。

【0104】復号化処理手段12は、情報ストリームを受信し、ユーザセルに記載されているVPI [11:0]を抽出する。そして、抽出したVPI [11:0]のVPI [11:4]をRAM11aへの読み出しアドレスとし、VPI [3:0]に対応する位置にあるビットのaビット情報を読み出しデータとする。aビット情

報=1ならば、そのセルを暗号鍵を用いてDechurnし、aビット情報=0ならば、NotDechurn（復号化を行わずスルー）とする。

【0105】図14は次フレームからDechurnを行う際のタイミングチャートを示す図である。情報ストリームのPLOAMセルaのChurned-VP設定情報に、VPI [11:0] = “001”（“001”はヘキサデータの）の情報がChurnされている（aビット情報=1）旨が記載されているものとする。

【0106】Churned-VPメッセージフラグ設定手段11-1は、PLOAMセルaを受信して、41バイト目のChurned-VP設定情報の1Dを認識すると、Churned-VPメッセージフラグを図に示す位相で出力する。

【0107】また、Churned-VP設定情報書き込み手段11-2は、VPI [11:0] = “001”及びaビット情報（=1）を次フレームのユーザセルC1の区間まで内部でラッチする。

【0108】そして、Churned-VPメッセージフラグとPLOAMパルス（PLOAMセルの位置を示すパルス）との論理をとった信号をライトイネーブルとして、図に示すセルFP（セルの位置を示すパルス）の位置で、VPI [11:4] = “00”をRAM11aの書き込みアドレス、16ビットのVPI [3:0] = “1”の位置にaビット情報を書き込みデータとしてRAM11aに書き込む。

【0109】このように、PLOAMセルaを受信した後、次フレームのPLOAMセルbの先頭位置でPLOAMセルaにあったChurned-VP設定情報をRAM11aに書き込み、その後、復号化処理手段12で読み出して、図に示す位置A（次フレームのユーザセルC1の先頭）からVPI [11:0] = “001”に対応するセルのDechurnを行っていく。ここではVPI [11:0] = “001”はセルC1としたので、位置AからセルC1のDechurnが行われる。

【0110】一方、情報ストリームのPLOAMセルbのChurned-VP設定情報に、VPI [11:0] = “010”とあり、Churnされていない（aビット情報=0）旨が記載されている場合には、図に示すようなタイミングでVPI [11:0] = “010”はNotDechurnとなる。

【0111】このように、本発明のONU10では、OLTがPLOAMセルに設定したChurned-VP設定情報を、次フレームにあるPLOAMセル以降から有効にするような構成とした。

【0112】これにより、次フレームのユーザセルから即時にDechurn処理を行うことができるので、暗号化処理と復号化処理の不一致防止、さらにデータ疎通時間を短縮させることが可能になる。

【0113】次に本発明の光加入者線端局装置について

説明する。図15は本発明の光加入者線端局装置の原理図である。光加入者線端局装置20は、ATM-PONのような光加入者系システムに接続し、暗号鍵を用いて、暗号化を行った情報部分を含む情報ストリームをONU30a~30n(総称してONU30)へ送信する。以降では、光加入者線端局装置20をOLT20と呼ぶ。

【0114】OLT20は、フラグ設定制御手段21と、暗号化設定情報送信制御手段22と、暗号化設定情報上書き手段23と、暗号化設定情報更新手段24から構成される。

【0115】フラグ設定制御手段21は、情報ストリームの送信時にONU30の装置状態等にもとづいて、フラグを設定する。暗号化設定情報送信制御手段22は、設定されたフラグにもとづいて、論理コネクション毎に暗号化を施したか否かを示す設定情報である暗号化設定情報(Churned-VP設定情報)の送信制御を行う。

【0116】暗号化設定情報上書き手段23は、Churned-VP設定情報をONU30へ再度送信する上書き処理を行う。暗号化設定情報更新手段24は、Churned-VP設定情報の更新タイミングを暗号化の更新周期終了時に一致させる。

【0117】次にフラグ設定制御手段21の初期暗号化(以下、初期Churn)フラグについて説明する。OLT20は、停止状態から運用状態(O8状態)へ移行したONU30aに対し、Churned-VP設定情報を送信する。ONU30が停止状態からO8状態へ移行した時に、Churned-VP設定情報を送信することを初期Churnと呼ぶ。

【0118】フラグ設定制御手段21では、初期Churnフラグを設けて、この初期Churnを実行する。初期Churnフラグの設定制御としては、ONU30が停止状態から初期Churnフラグをクリアし(Oとし)、初期Churn完了で初期Churnフラグをセットする(1とする)。

【0119】暗号化設定情報送信制御手段22は、ONU30がO8状態へ移行した時に、この初期Churnフラグをチェックし、初期Churnフラグがセットされていない場合は、初期Churnを実行する。

【0120】図16は初期Churnフラグを用いた初期Churn処理手順を示すフローチャートである。なお、ONUには固有の番号nが与えられており、ONUの装置状態と後述する各種のフラグはnで管理される。

【S60】フラグ設定制御手段21は、ONU(n)が停止状態の場合に初期Churnフラグ(n)を0とする。

【S61】ONU(n)が停止状態からO8状態へ移行する。

【S62】フラグ設定制御手段21は、O8状態に遷移

したONU(n)が、初期Churnフラグ(n)が0であるか否かを判断する。0ならばステップS63へ行き、1ならば初期Churn完了とみなして終了する。

【S63】暗号化設定情報送信制御手段22は、初期Churnを実行する。ここで、初期Churnでは、ONU(n)に対して、4096VP分のChurned-VP設定情報を送信する。ONU(n)に対して、4096VP分のChurned-VP設定情報の送信が完了し、ONU(n)からメッセージ正常受信を通知するAckを、4096VP分受信すると初期Churnは完了となり、初期Churnフラグ(n)を1とする。

【0121】以上説明したように、初期Churnフラグを設けて、初期ChurnフラグをONU30が停止状態でクリア、初期Churnの完了時にセットすることにした。

【0122】これにより、ONU30が停止状態からO8状態へ移行した時だけに初期Churnを実行することができ、他の状態から移行した時には初期Churnを実行せず、無駄な処理を省くことが可能になる。

【0123】次にフラグ設定制御手段21の初期Churn実行中フラグについて説明する。初期Churnを行う場合には、初期Churn実行中フラグを設け、初期Churnの実行中はこの初期Churn実行中フラグをセットする。そして、初期Churn実行中フラグがセットされている場合は、次の初期Churn要求を受け付けないこととする。

【0124】すなわち、複数のONUが連続して停止状態からO8状態へ移行した場合などに対し、最初に停止状態からO8状態へ移行したONUに対して初期Churnを開始し、その時に初期Churn実行中フラグをセットして、その他のONUは待機させる。

【0125】そして、実行中のONUの初期Churnが完了すれば、待機しているONUの初期Churnを開始していく。図17は初期Churn実行中フラグを用いた初期Churn処理手順を示すフローチャートである。

【S70】フラグ設定制御手段21は、初期Churnフラグ(n)が0であることを確認する。

【S71】フラグ設定制御手段21は、初期Churn実行中フラグが0であるか否かを判断する。初期Churn実行中フラグが0であればステップS72へ、1であればステップS74へ行く。

【S72】フラグ設定制御手段21は、他のONUが初期Churn実行中ではないため、初期Churn実行中フラグを1とする。

【S73】暗号化設定情報送信制御手段22は、該当するONU(n)に対して初期Churnを行う。

【S74】暗号化設定情報送信制御手段22は、初期Churn実行中フラグが0になるまで(先行する初期C

hurnが終了するまで)、初期Churnを待機する。

【0126】以上説明したように、初期Churn実行中フラグが0である場合にのみ、対応するONUに対して初期Churnを行い、先行する初期Churnが終了した場合に、次のONUに対して初期Churnを行う構成とした。

【0127】これにより、複数のONUから連続で初期Churn要求が発生しても、初期ChurnをONU単位のシリアル処理として行うことができるので、複雑な輻輳処理をすることなく、効率よく初期Churnを行うことが可能になる。

【0128】次にフラグ設定制御手段21の設定更改失敗フラグについて説明する。初期Churnが完了したONUの運用中に、OLT20がChurned-VP設定情報の設定更改(設定変更)や上書き処理などを行った時に、ONU30へのChurned-VP設定情報の設定が失敗したとする。

【0129】このような、Churned-VP設定情報の設定更改失敗(LOAI(Churn))が原因で状態落ち(停止状態へ遷移すること)が発生した場合は、再度、Q8状態へ遷移した時に初期Churnを実行する必要がある。

【0130】そこで、フラグ設定制御手段21では、ONU30の運用中にChurned-VP設定情報の設定失敗の有無を示す設定更改失敗フラグを設ける。暗号化設定情報送信制御手段22は、設定更改失敗フラグがセットされている場合には、Churned-VP設定情報の設定更改に失敗したものとみなして、該当するONU30に対して初期Churnを実行する。

【0131】なお、以降の説明では、初期Churnが完了した運用中のONUに対して、Churned-VP設定情報の更改を行う場合の処理を、設定更改Churnと呼ぶ。

【0132】図18は設定更改失敗フラグを用いた初期Churn処理手順を示すフローチャートである。

【S80】フラグ設定制御手段21は、Churned-VP設定情報を送信した後、例えば、300ms以内にONU(n)からメッセージ正常受信を示すAckを受信しない場合、設定失敗とみなして、設定更改失敗フラグ(n)を1にする。

【S81】暗号化設定情報送信制御手段22は、ONU(n)に対する各種メッセージの送信を中断する。ONU(n)は停止状態となる。

【S82】暗号化設定情報送信制御手段22は、設定更改失敗フラグ(n)が1となっているONU(n)が、再度Q8状態へ遷移した時に、あらためて初期Churnを実行する。

【0133】以上説明したように、ONU30に対して設定更改Churnが失敗した場合には、設定更改失敗

フラグを1として、再度初期Churnを行う構成とした。これにより、設定更改Churnの失敗時に、再度初期Churnを行って、Churned-VP設定情報を送信できるので、OLT20とONU30とのChurned-VP設定情報の設定不一致を防止することが可能になる。

【0134】次にフラグ設定制御手段21の設定更改未完了フラグについて説明する。初期Churnを完了したONU30が、設定更改Churn失敗以外の何らかの要因で状態落ちした場合には、Churned-VP設定情報の設定更改が終了していないことになる。そこで、フラグ設定制御手段21では、設定更改未完了フラグを設け、終了していない場合は、設定更改未完了フラグをセットする。

【0135】そして、暗号化設定情報送信制御手段22は、該当するONUが再度Q8状態へ遷移した時に、設定更改未完了フラグをチェックし、フラグがセットされていれば初期Churnを実行する。

【0136】図19は設定更改未完了フラグを用いた初期Churn処理手順を示すフローチャートである。

【S90】ONU(n)が状態落ちした場合は、設定更改が未完了であることを示す設定更改未完了フラグ(n)を1とする。

【S91】暗号化設定情報送信制御手段22は、ONU(n)に対する各種メッセージの送信を中断する。ONU(n)は停止状態となる。

【S92】暗号化設定情報送信制御手段22は、設定更改未完了フラグ(n)が1となっているONU(n)が、再度Q8状態へ遷移した時に、あらためて初期Churnを実行する。

【0137】以上説明したように、ONU30の状態落ちが発生した場合には、設定更改未完了フラグを1として、再度初期Churnを行う構成とした。これにより、設定更改Churn失敗以外の場合でも、再度初期Churnを行って、Churned-VP設定情報を送信できるので、OLT20とONU30とのChurned-VP設定情報の設定不一致を防止することが可能になる。

【0138】次にフラグ設定制御手段21のChurn更改中フラグについて説明する。Churn更改周期の期間中に、設定更改Churn等(上書き処理も含め)を行うと、Churn更改と設定更改Churnが輻輳する可能性があるが、設定更改Churnが正常に行われない場合がある。

【0139】したがって、フラグ設定制御手段21は、Churn更改フラグを設け、Churn更改周期中はこのフラグをセットする。Churn更改中フラグがセットしている期間(OLT20から送信されるメッセージの送信禁止期間となる)に、ONU30からChurned-VP設定情報の更改要求等があった場合は、要

求をwaitさせ、Churn更改終了後に設定更改Churnを実行する。これにより、OLT20とONU30とのChurned-VP設定情報の設定不一致を防止することが可能になる。

【0140】次にフラグ設定制御手段21の設定更改要求フラグについて説明する。初期Churnが完了した運用中のONUに対し、OLT20が設定更改Churnを行う場合は、外部の保守端末装置よりONU単位に設定更改要求フラグをOLT20にセットする。

【0141】OLT20は、設定更改要求フラグがセットされたONUに対し、設定更改Churnを行う。設定更改Churn完了で設定更改要求フラグをクリアする。これにより、初期Churnで設定したChurned-VP設定情報をO8状態中に更新することが可能になる。

【0142】一方、設定更改要求フラグは、ONU単位とし、1回の設定更改で1ONUにつき1VPIの更改に制限する。このため、同線のVPIの設定更改の場合には、すべてのONUに対し同一設定ができる。

【0143】また、1ONUにつき1VPIと制限することで、1回の設定更改Churnは、Churn更改周期内で完了できるため、Churn設定更改処理時間を明確に規定できる。

【0144】次にフラグ設定制御手段21の設定更改実行中フラグについて説明する。設定更改Churnは、Churned-VP設定情報の設定更改処理であるため処理の優先順位が高い。そこで設定更改実行中フラグを掛け、実行中はこのフラグをセットする。

【0145】設定更改実行中フラグのセット中は、他のONUからの要求をwaitさせることで割り込みを防止し、Churn設定更改の処理の優先順位を高くする。次に設定更改Churnの処理手順について図20～図23を用いて説明する。図20、図21は設定更改Churn開始時の処理手順を示すフローチャートである。

【S100】暗号化設定情報送信制御手段22は、設定更改要求フラグが1か否かを判断する（配下のONU30a～30nの1ONUでも設定更改要求があるか否かを判断する）。1ならばステップS101へ、0ならば終了する。

【S101】暗号化設定情報送信制御手段22は、SENDフラグ（フラグ設定制御手段21は、OLT20がChurned-VP設定情報を送信している場合は、SENDフラグをセットする）をチェックする。

【0146】SENDフラグが1であれば0になるまで待機し（ステップS101を繰り返す）、SENDフラグが0ならばステップS102へ行く。

【S102】フラグ設定制御手段21は、SENDフラグをあらためて1にセットして、その他の要求を受け付けないようにする。

【0147】ここで、ステップS103以降から並列処理となる。例えば、ONU30a、30b及び30cに対して設定更改要求があったものとする、ONU30a、30b及び30cの3つの並列処理が行われる。以降では、ONU30aに対する設定更改Churnの処理を説明する。

【S103】フラグ設定制御手段21は、設定更改要求フラグを0にする。

【S104】フラグ設定制御手段21は、設定更改実行中フラグを1にする。

【S105】暗号化設定情報送信制御手段22は、Churned-VP設定情報に更改VPIをセットし、Churned-VP設定情報の送信回数k（例えば、k=3）を設定する。

【S106】暗号化設定情報送信制御手段22は、Churn更改中フラグが1か否かを判断する。1の場合は0になるまで待機し（ステップS106を繰り返す）、0の場合はステップS107へ行く。

【S107】ONU30aがO8状態から状態落ちしたか否かを判断する。すなわち、設定更改未完了フラグをチェックし、フラグが1ならばステップS110へ行き、フラグが0ならばステップS108へ行く。

【S108】暗号化設定情報送信制御手段22は、Churned-VP設定情報を送信し、Churned-VP設定情報を1回送信する度にkから1をデクリメント（k=k-1）、送信回数を管理する。

【S109】k=0ならば終了し、k≠0ならばステップS106へ戻る。

【S110】暗号化設定情報送信制御手段22は、初期Churnを行う。

【0148】図22はACKメッセージの受信処理時のフローチャートを示す図である。OLT20がChurned-VP設定情報を送信した場合、ONU30aが正常にChurned-VP設定情報を受信すると、ACKメッセージをOLT20へ返送する。

【S120】暗号化設定情報送信制御手段22からChurned-VP設定情報の送信後（例えば、3回送信した後）、一定時間内（例えば、300ms以内）でACKメッセージの返答があるか計測する。タイムアウトした場合はステップS123へ、そうでなければステップS121へ行く。

【S121】Churn更改中フラグが1か否かを判断する。1の場合は0になるまで待機し（ステップS121を繰り返す）、0の場合はステップS122へ行く。

【S122】フラグ設定制御手段21は、設定更改実行中フラグを0にする。

【S123】フラグ設定制御手段21は、設定更改失敗フラグを1にする。

【S124】暗号化設定情報送信制御手段22は、初期Churnを行う。

【0149】図23は設定更改Churn終了時のフローチャートを示す図である。

【S130】すべてのONUの設定更改実行中フラグを監視し、設定更改実行中フラグがすべて0ならば、処理完了となりステップS131へ行く。そうでなければ0になるまで設定更改実行中フラグを監視し続ける（ステップS130を繰り返す）。

【S131】SENDフラグを0にして、他の処理に放す。

【0150】次に暗号化設定情報上書き手段23について説明する。初期Churn完了後、Churned-VP設定情報の設定更改がなければ、その後、OLT20がONU30に対してChurned-VP設定情報を送信することはない。

【0151】このため、従来では何らかの原因で、OLT20とONU30とのChurned-VP設定情報が設定不一致となった場合でも不一致となった状態を確認することができなかった。

【0152】そこで、本発明では暗号化設定情報上書き手段23を設け、ONU30が運用中、初期Churn完了をトリガとして、Churned-VP設定情報の上書き処理である上書きChurnを実行させることにした。これにより、何らかの原因でOLT20とONU30とのChurned-VP設定情報が設定不一致となった場合でも、上書きChurnで一致させることができる。

【0153】また、上書きChurnは、OLT20とONU30とのChurned-VP設定情報を一致させるための保護機能であるため、処理の優先順位は低くて構わない。

【0154】そこで、上書きChurnのChurned-VP設定情報に対する送信要求は、他のメッセージ送信要求がある場合や設定更改Churnを行っている等の場合はwaitさせて、上書きChurnの優先順位を低くする。これにより、他のメッセージ送信を圧迫せずに、上書きChurnを実行できる。

【0155】さらに、暗号化設定情報上書き手段23の内部には、上書きChurnを実行するためのタイマが設けられる。このタイマは、上書きChurn用のChurned-VP設定情報の送信後に起動し、上書きChurnを行うべき最低限の周期を計測する。

【0156】そして、タイマで計測された次の送信時刻（他のメッセージ送信と競合しないように設定される）がくるまでは、上書きChurn用のChurned-VP設定情報は送信しない。

【0157】また、タイマの設定周期は、保守端末装置を通じて、任意の値を設定できる。したがって、上書きChurn設定に柔軟性を持たせることができる。次にChurning-Keyアップデートメッセージと、Churned-VP設定情報との送信時の競合防止に

ついて説明する。

【0158】ITU-T勧告G.983では、ONU30へのメッセージは、一定周期に発生する下りPLOAMセルにより送信される。したがって、PLOAMセル周期で送信すべきメッセージの調停処理を行って、ONU30へ送信するメッセージを決定しなければならない。

【0159】Churning-Keyアップデートメッセージは、図5で上述したように16×Tフレーム間隔で送信される。また、Churned-VP設定情報は、Churn更改中フラグがセットされていない間、3回の送信を完了する必要がある。

【0160】暗号化設定情報送信制御手段22は、Churning-Keyアップデートメッセージと、Churned-VP設定情報との調停処理を行った場合には、Churning-Keyアップデートメッセージを優先する。

【0161】すると、Churning-Keyアップデートメッセージは、16×Tフレーム間隔に自動的に送信される。その後、Churned-VP設定情報が例えば16×Tフレーム間隔で3回自動的に送信される。

【0162】すなわち、Churning-Keyアップデートメッセージと、Churned-VP設定情報の初回のみが調停対象となり、初回のChurning-Keyアップデートメッセージが送信されれば2回目、3回目のメッセージ送信は互いに競合を起こすことなく自動的に送信することが可能になる。

【0163】次に暗号化設定情報更改手段24について説明する。ITU-T勧告G.983では、Churning-Key更改タイミングは規定されているが、Churned-VP設定情報の更改タイミングは規定されていない。このため、OLT20ではChurned-VP設定情報に対して、不規則に設定情報の更改を行うと、OLT20とONU30とのChurned-VP設定情報の設定不一致を起こしてしまう可能性がある。

【0164】そこで、暗号化設定情報更改手段24は、Churning-Key更改タイミングでChurned-VP設定情報の更改を行うことにして不一致を防止する。

【0165】図24はChurned-VP設定情報の更改を示す図である。Churned-VP設定情報を3回送信完了後の最初のChurning-Key更改タイミングtで、送信されたChurned-VP設定情報に対する設定更改を行っていく。

【0166】これにより、OLT20とONU30間でChurned-VP設定情報の設定更改を同期して行うことが可能になり、Churned-VP設定情報の設定不一致を防止することが可能になる。

【0167】

【発明の効果】以上説明したように、本発明の光加入者線終端装置は、現在使用中の暗号化設定情報を記憶するアクティブ側の第1の記憶手段と、新しく更改された暗号化設定情報を記憶するバックアップ側の第2の記憶手段との切り替え制御を行い、読み出した暗号化設定情報にもとづいて、次フレームの先頭から暗号化された情報部分の復号化処理を行う構成とした。これにより、暗号化設定情報の送信側と受信側との暗号化・復号化の処理タイミングのずれを防止し、高品質な通信制御を行うことが可能になる。

【0168】また、本発明の光加入者線端局装置は、受信装置へ情報ストリームを送信する際に、フラグの設定制御を行い、フラグにもとづいて、暗号化設定情報の送信制御を行う構成とした。これにより、暗号化設定情報の送信側と受信側との暗号化・復号化の処理タイミングのずれを防止し、高品質な通信制御を行うことが可能になる。

【図面の簡単な説明】

- 【図1】 本発明の光加入者線終端装置の原理図である。
- 【図2】 情報ストリームの構成及びChurned-VP設定情報のフォーマットを示す図である。
- 【図3】 Churning-Keyの更改シーケンスを示す図である。
- 【図4】 2面RAMを持つONUのブロック構成を示す図である。
- 【図5】 コピー動作手順を示すフローである。
- 【図6】 コピー動作時のタイミングチャートを示す図である。
- 【図7】 コピー中にChurned-VP設定情報を受信した際の動作を示すタイミングチャートである。
- 【図8】 応答信号の返送制御手順を示すフローチャートである。
- 【図9】 更改されたChurned-VP設定情報をSRAMから不揮発性メモリへ記憶させる場合の処理手順を示すフローチャートである。
- 【図10】 暗号化設定情報記憶手段の電源復旧時の動作状態を示すフローチャートである。
- 【図11】 復号化マスク処理を示す図である。
- 【図12】 ONUの変形例を示す図である。

【図13】 次フレームでDechurnを実現するためのブロック構成を示す図である。

【図14】 次フレームからDechurnを行う際のタイミングチャートを示す図である。

【図15】 本発明の光加入者線端局装置の原理図である。

【図16】 初期Churnフラグを用いた初期Churn処理手順を示すフローチャートである。

【図17】 初期Churn実行中フラグを用いた初期Churn処理手順を示すフローチャートである。

【図18】 設定更改失敗フラグを用いた初期Churn処理手順を示すフローチャートである。

【図19】 設定更改未完了フラグを用いた初期Churn処理手順を示すフローチャートである。

【図20】 設定更改Churn開始時の処理手順を示すフローチャートである。

【図21】 設定更改Churn開始時の処理手順を示すフローチャートである。

【図22】 ACKメッセージの受信処理時のフローチャートを示す図である。

【図23】 設定更改Churn終了時のフローチャートを示す図である。

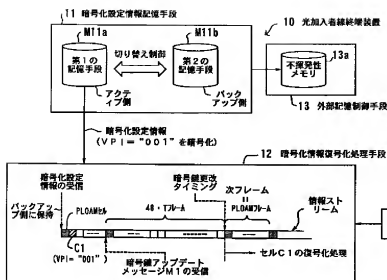
【図24】 Churned-VP設定情報の更改を示す図である。

【図25】 ATM-PONシステムの構成を示す図である。

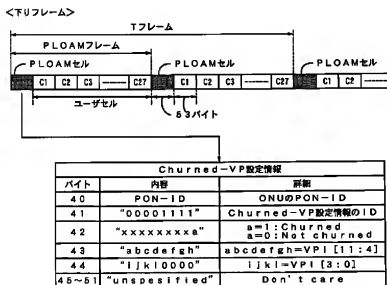
【符号の説明】

- 10 光加入者線終端装置
- 11 暗号化設定情報記憶手段
- 12 暗号化設定情報復号化処理手段
- 13 外部記憶制御手段
- 13a 不揮発性メモリ
- 14 復号化マスク手段
- M11a 第1の記憶手段
- M11b 第2の記憶手段
- 【手続補正2】
- 【補正対象書類名】 図面
- 【補正対象項目名】 全図
- 【補正方法】 変更
- 【補正内容】

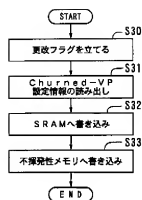
【図1】



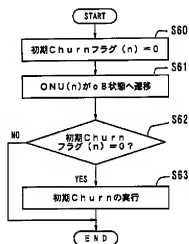
【図2】



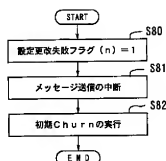
【図9】



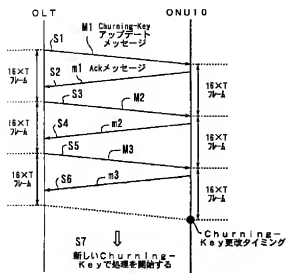
【図16】



【図18】

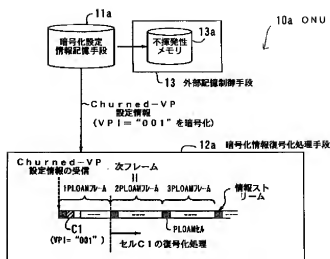


【図3】

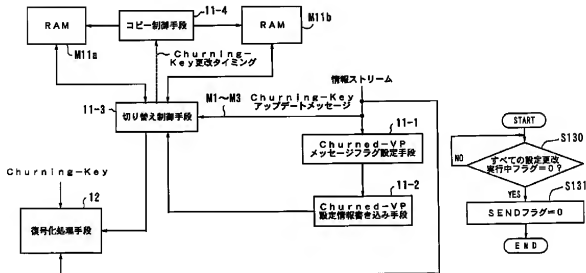


【図4】

【図12】



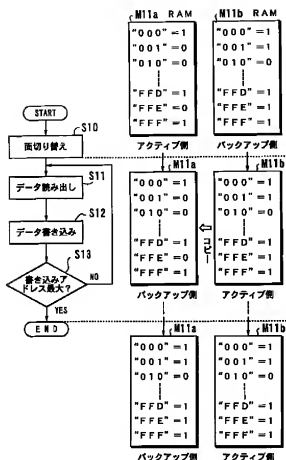
【図23】



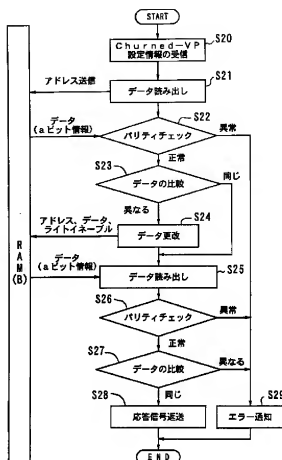
【図7】



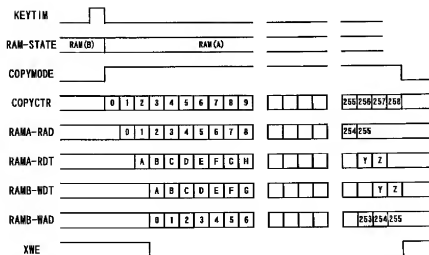
【図5】



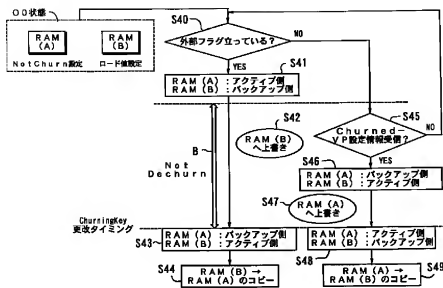
【図8】



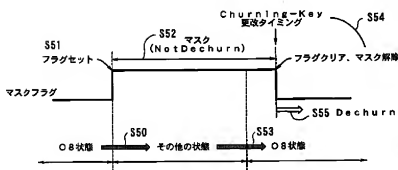
【図6】



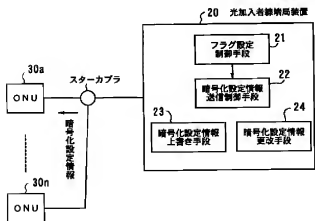
【図10】



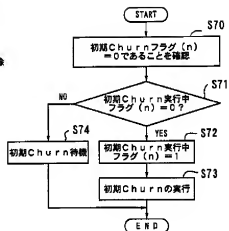
【図11】



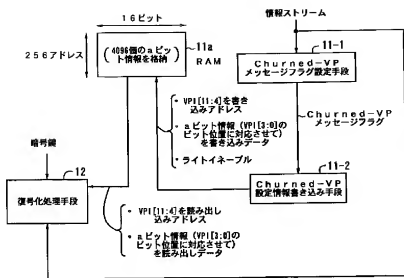
【図15】



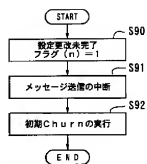
【図17】



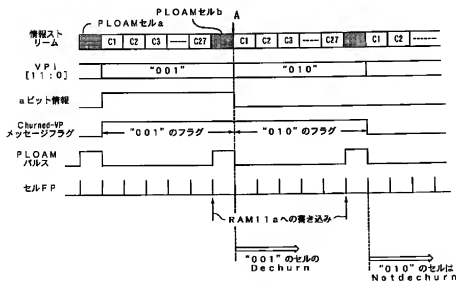
【図13】



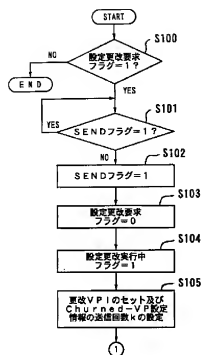
【図19】



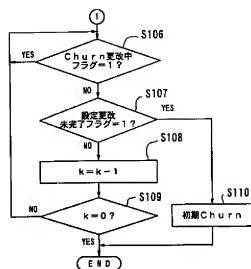
【図14】



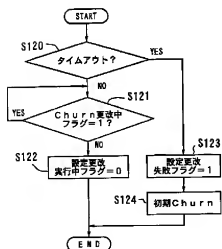
【図 20】



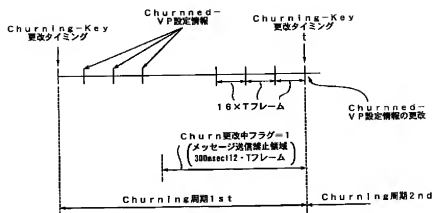
【図 21】



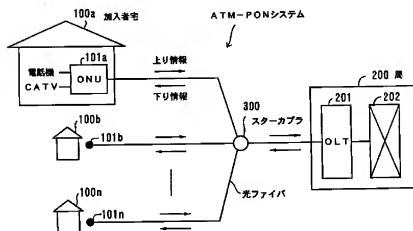
【図 22】



【図24】



【図25】



フロントページの続き

(51) Int. Cl. ⁷

H04Q 11/04

識別記号

F I

H04Q 11/04

データベース (参考)

B 9A001

(72) 発明者 三浦 健司

大阪府大阪市中央区城見2丁目2番6号
富士通関西デジタル・テクノロジー株式会社
社内

(72) 発明者 塩野 秀樹

大阪府大阪市中央区城見2丁目2番6号
富士通関西デジタル・テクノロジー株式会社
社内

(72) 発明者 松尾 保

大阪府大阪市中央区城見2丁目2番6号
富士通関西デジタル・テクノロジー株式会社
社内

(72) 発明者 豊田 好美

大阪府大阪市中央区城見2丁目2番6号
富士通関西デジタル・テクノロジー株式会社
社内

(72)発明者 小柳 敏則
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 阿比留 節雄
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 安里 淳
大阪府大阪市中央区城見2丁目2番6号
富士通関西デジタル・テクノロジー株式会
社内

(72)発明者 藤吉 新一
福岡県福岡市博多区博多駅前三丁目22番8
号 富士通九州デジタル・テクノロジー株
式会社内

(72)発明者 内田 和宏
福岡県福岡市博多区博多駅前三丁目22番8
号 富士通九州デジタル・テクノロジー株
式会社内

(72)発明者 龍 一也
福岡県福岡市博多区博多駅前三丁目22番8
号 富士通九州デジタル・テクノロジー株
式会社内

(72)発明者 平島 勝彦
福岡県福岡市博多区博多駅前三丁目22番8
号 富士通九州デジタル・テクノロジー株
式会社内

(72)発明者 四丸 建夫
福岡県福岡市博多区博多駅前三丁目22番8
号 富士通九州デジタル・テクノロジー株
式会社内

(72)発明者 若古 光春
福岡県福岡市博多区博多駅前三丁目22番8
号 富士通九州デジタル・テクノロジー株
式会社内

(72)発明者 酒井 俊行
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

Fターム(参考) 5J104 AA01 AA16 AA34 NA02 NA37
PA00 PA06
5K002 AA03 AA04 DA05 DA12 EA03
FA01
5K030 GA11 GA15 HA10 HB14 JA08
JL03 JL08 KA04 KA13 KA21
LA07 LA12 LE05 MC07 MD02
5K033 AA05 AA07 AA08 CB15 CB17
DA15 DB10 DB12 DB22 EB06
5K069 AA10 BA10 CA02 CB01 CB05
DA06 EA11 EA24 FC06 HA09
9A001 BB02 BB03 BB04 CC04 CC07
DD08 DD10 EE03 JJ18 JJ20
KK16 KK43 KK56 LL02 LL03
LL05